MICRO FOCUS®

Reflection Desktop
Help

Version 17.0 SP1

Contents

3   How Do I?   55

7 Printing   553

8 Creating and Using Macros   653

9 File and Data Transfer

10 Reflection FTP Client

Introduction

Welcome to Reflection Desktop, a full-featured desktop application that allows you to run host applications, transfer files, and integrate host data into the latest Windows and Office software applications. For more about Reflection Desktop, see "Reflection Desktop Features" on page 14.

To find information about...	See these topics in this guide	And this content on the Web
Installing and using Reflection	◆ Chapter 2, "Get Started," on page 21 ◆ Chapter 1, "Installation," on page 17	Reflection Desktop Evaluation Guide User Videos
Configuring and deploying Reflection	◆ Chapter 3, "How Do I?," on page 55 ◆ The User Interface ◆ Terminal Sessions ◆ Chapter 6, "Secure Connections," on page 425	Reflection Desktop Deployment Guide Deployment Videos Reflection Desktop 17.0 Release Notes
Setting up file transfers	◆ File and Data Transfer ◆ Reflection FTP Client	
Programming with the Reflection APIs	◆ "Record, Run, and Edit VBA Macros" on page 88 ◆ Using Macros Created with other Products	The Reflection Desktop .NET Programming Guide The Reflection Desktop VBA Guide **NOTE:** These guides are also available on the Help menu when the VBA or .NET features are installed.

What's New

Reflection Desktop v17.0 SP1 includes several major new features, enhancements, and installation requirements:

IT Administration Features

This release supports the latest Windows 10 "Windows as a Service" update.

Reflection X Advantage improvements:

◆ Reflection X Advantage now provides a new, modern installer for Linux systems.

File Transfer

Reflection Desktop 17.0 SP1 now supports BIFF and BIFF8 file transfer methods on IBM System i systems. Other versions (including IBM AS/400, AS400, and iSeries systems) are also supported.

Reflection Desktop Features

With Reflection providing terminal emulation, you can use your PC to connect to:

- An IBM mainframe as a 3270 terminal or 3287 printer, using Telnet or Telnet Extended (TN3270/E).
- An IBM System i midrange computer as a 5250 terminal or 3812 printer, using Telnet (TN5250/E).
- A UNIX or Open VMS host, using a variety of connection methods.

You can start multiple terminal sessions and even Web pages in a single workspace the same way you'd open multiple documents in most applications.

If you've previously used Reflection or Extra! for product emulation, you'll find many new features in Reflection Desktop. These features combine the best emulation features of Reflection and Extra! into a single solution, optimized for Microsoft Windows 7, Windows 8.1, Windows 10, and Microsoft Office.

NOTE: Depending on the version of Reflection you have installed, the details of your license agreement, and the security settings applied by your system administrator, some connection types and features described in this Guide may not be available to you.

Following is a summary of the many new and enhanced user interface, productivity, management, and security features you'll find in Reflection.

- **User Interface**

  You can choose from five types of user experiences: Ribbon, Browser, Classic, Classic MDI, or TouchUx. The Reflection Ribbon has the look and feel of Microsoft Office, including integrated search and theme support. The Reflection Browser has a look and feel similar to the latest Web browsers where screen real estate is maximized. The Classic interface is similar to the Extra! X-treme and legacy Micro Focus Reflection terminal emulation applications. The Classic MDI option is similar to the Classic option. (Unlike Classic, it provides a multi-document interface that allows more than one document to be open in a workspace.) And the TouchUx interface provides a touchscreen user experience with an iOS, Android or Windows 8 look and feel.

  The Ribbon, Browser, and TouchUx interfaces provide a multiple document interface, in which you can open multiple sessions. These interfaces also allow you to view and interact with Web pages within the Reflection workspace.

- **Productivity Tools**

  Tightly integrated with Microsoft Office, Reflection supports productivity features such as Recent Typing, Scratch Pad, Auto Complete, Auto Expand, Spell Check, and Screen History to drive user efficiency. If Microsoft Office 2007 or later is installed, you can leverage host data in e-mail messages, contacts, appointments, notes, tasks, and word-processing documents.

- **Management**

  You can create and distribute customized 3270, 5250, 6530, and VT session documents that include host specifications, or add Web pages to your workspace or layout. Session documents include pointers to mouse maps, keyboard maps, theme files, hotspot files, and Ribbons that you can use to customize the behavior of the session. You can further customize each session by adding macros, scripts, executables, and other options to context menus.

You can connect to hosts that use IP version 6 (IPv6) addresses. And, you can specify a backup host to which Reflection automatically connects in case of connection failure or interruption.

License metering for Reflection Desktop is available through the optional Reflection Security Gateway and its administrative console.

⬥ **Security Services**

Reflection provides the following security features for determining who can access and use sensitive host data.

- ⬥ **User Account Control (UAC) for Installation** — Build Microsoft Installer (.msi) packages and lock down features.

- ⬥ **Online Certificate Revocation** — When making secure connections, check the authenticity of certificates using Online Certificate Status Protocol (OCSP), a faster alternative to checking Certificate Trust Lists (CTL).

- ⬥ **Trusted Locations** — Prevent security problems by allowing users to open documents only from trusted locations that you specify in the **Trust Center**.

- ⬥ **Expanded Information Privacy Support** — Protect credit/debit card primary account numbers or other sensitive data that is entered or stored on host screens or in productivity features, such as Screen History.

To reinforce mainframe security, you can add a layer of protection in front of the host with secure token authorization, using the optional Reflection Security Gateway.

⬥ **Automation and Developer Support**

Using the Reflection object-oriented API model, add functionality to terminal sessions and Web pages using .NET API, Visual Basic for Applications (VBA), or HLLAPI programming. You can also create and run VBA scripts using functions provided by the VBA development environment. Documentation for the .NET API and VBA are provided from the Help button on the workspace frame.

Layout files give you the ability to access the Reflection .NET API in multiple instances of Reflection simultaneously. API security settings allow you to control access to the application through API or macro calls.

⬥ **Legacy Support**

Reflection Desktop protects the investment you've made in previous products.

You can run sessions you created in Extra!, KEA!, IBM Personal Communications, and Micro Focus Rumba.

You can also still run and edit the macros and scripts you created in Extra! and legacy Reflection, including encrypted Extra! macros. And Reflection supports most types of macros created in Micro Focus Rumba, OpenText HostExplorer, IBM PComm, and Brandon Systems\Jolly Giant QWS3270.

Related Topics

1 Installation

You can install Reflection from a downloaded distribution, an administrative installation image, or from a CD. If you are an administrator looking for instructions on how to create a customized installer, see the Reflection Deployment Guide.

NOTE: Reflection is typically distributed electronically. If your installation requires a CD, you will need to request it when you place your order.

In this Chapter

Upgrading from Previous Versions

When you install Reflection Desktop, it upgrades the following Micro Focus products:

- Reflection for IBM 2007, 2008, 2011, and 2014
- Reflection for UNIX and OpenVMS 2008, 2011, and 2014
- Reflection for IBM v. 8.0 - 14.x
- Reflection for UNIX and OpenVMS v. 8.0 - 14.x
- Reflection for the Multi-Host Enterprise, Standard Edition v. 8.0 - 14.x
- EXTRA! X-treme v. 8.0 - 9.3
- Extra! X-treme v. 9.4 or greater
- myEXTRA! Enterprise v. 7.0
- myEXTRA! v. 7.x
- EXTRA! Enterprise 2000

NOTE: Reflection 2007, 2008, 2011, and 2014 are automatically removed when you upgrade. Extra! and the other Reflection products are automatically removed when you upgrade using setup.exe. If you upgrade these products by deploying the .msi file directly, you will get a message telling you to uninstall the older software first.

Supported Reflection Configuration Files

Reflection Desktop represents an upgrade over previous versions of both Reflection and Extra!. Most configuration files used with these products are supported by the new version.

For a complete list of Extra! and legacy Reflection files supported by Reflection Desktop, see Knowledge Base Article 7021411 (https://support.microfocus.com/kb/doc.php?id=7021411).

Related Topics

- "Install Reflection on a Workstation" on page 18

Install Reflection on a Workstation

NOTE: You must log on with administrator privileges to install Reflection. If you do not have the necessary access rights, ask your system administrator to elevate your privileges.

To install on a workstation

1 Run the Reflection Setup program.

If you install from	Do This
A download site	Click the download link, and then run the download program. Select a location for the installer files, and then click Next. This extracts the files to the specified location and starts the Reflection Setup program.
An administrative installation image	From the administrative installation point, double-click the `setup.exe` file.

2 From the Reflection Setup program, click **Continue**, and then accept a license.

3 (Optional) To change the default installation folder, click the **File Location** tab and browse to the folder in which you want to install Reflection.

4 (Optional) To select which features, components, or languages are installed, click the **Feature Selection** tab.

5 Click **Install Now**.

NOTE: Use the **Advanced** tab of the installer only if you want to modify the installer log settings, or if you are an administrator configuring a Reflection deployment. An administrative installation does not actually install the product — instead, it creates an installation image that administrators can use to customize and deploy Reflection to end users.

Features Selection Tab

Use the **Feature Selection** tab to select which features you want to install.

Click the icon to the left of the feature name and select from the options below.

Option	Description
Feature will be installed on local hard drive	Installs the selected feature.
	NOTE: Some features listed under a selected feature may not be included when you select to install the higher-level feature. The features that are included are the recommended defaults. If you select the higher level feature a second time, all sub-features will be included.
Feature will be installed when required	Installs the feature when you first use it (for example, when you click the **Start** menu shortcut for this feature).
Feature will be unavailable	Leaves the feature uninstalled.

Set Your User Data Directory

You can specify any location as the user data directory. The default directory is Documents\Micro Focus\Reflection\.The directory you specify will be added as a Trusted Location.

To set the user data directory

1   Run the Reflection Setup program as shown in .

2   On the Reflection Setup program, click **File Location**, and then under **Default user data directory**, browse to the directory you want to use.

NOTE: This change only affects those features that you include in your initial installation. If you add a feature later using Programs and Features (or Add/Remove Programs), that application will use the original default directory (`Documents\Micro Focus\Reflection\`), not the value you specified for **Default user data directory**.

Advanced Tab

Use the **Advanced** tab of the installer only if you want to modify the installer log settings or you are an administrator configuring a Reflection deployment.

Install to this PC	Installs Reflection to your computer.
Create an Administrative install image on a server	**NOTE:** An administrative install image does not actually install the product — instead, it creates an installation image that administrators can use to deploy Reflection to end users.
	When you create an administrative install image, an image of Reflection is copied to a network location for later installation to multiple workstations. This network location can be used by deployment tools to access and create packages that are deployed to workstations. Also, end users can perform installations by running `setup.exe` from this location.

Log file settings

By default, an installation log file is created and then deleted after installation successfully completes. (This configuration avoids accumulation of large log files after successful installations.) To save a log file for all installations, including successful ones, select **Create a log file for this installation**, and clear **Delete log file if install succeeds**.

The installation log file, which provides details about the installation, is saved in the user's Windows temporary folder (`%tmp%`) with a generated name that begins with `atm`. To open this directory, launch the **Start** menu **Run** command and enter `%tmp%`.

2 Get Started

To get started with Reflection, use these instructions that show how to:

In This Section

- Connect to Hosts and the Web shows how to connect to a session and save your connection data in a session document file that you can reuse later.
- Get Familiar with the Reflection Interface describes the alternate Reflection interfaces and gives you some tips for getting around.
- Cut and Paste Show options for cutting and pasting screen data.
- Capture Screen History Shows how to capture screens as images or text and then export them to presentations, Word, or simple text files.
- Work with More than One Session Shows how to work with two or more sessions.
- "Get Started" on page 21 shows Extra! users how to get started with setting up terminal sessions in Reflection.

Videos

- ▶️ Working with Sessions (1:32)
- ▶️ Using the Reflection Ribbon (2:41)
- ▶️ Using Screen History (1:42)
- ▶️ Creating Training with Screen History (1:10)

Connect to Hosts and the Web

Using Reflection, you can connect to hosts and Web URLs directly from your desktop. If your enterprise uses a centralized management server, you can connect to sessions through that server. to make and control connections, you'll need to:

In this Topic

- "Connect and Save your Connection Settings" on page 22
- "Open a Terminal Session" on page 23
- "Connect or Disconnect a Session" on page 23
- "Open a Web Session" on page 23

Video

▶️ Working with Sessions (1:32)

Connect and Save your Connection Settings

To access a host, you need to open a session on that host. In Reflection, you can create a session document that allows you to configure and reuse your session.

Terminal sessions are pre-configured to use built-in Ribbon, theme, keyboard map, and mouse map files. If you choose, you can create custom versions of these files to modify the appearance and capabilities of each session.

CAUTION: If you specify a custom file for a session, be sure to maintain the same file name and file path (relative to the session document file) when you deploy the files. If Reflection cannot find the custom file when it starts a session, it prompts to use a built-in file.

To create a new terminal session and save your connection settings

1 Open Reflection.

2 If Reflection is set up to open the Create New Document dialog box automatically, you can skip this step. If this dialog box is not displayed, open it as follows:

The steps depend on your .

User Interface Mode	Steps
Ribbon or Reflection Browser	From the Quick Access Toolbar, click the **New Document** button.
TouchUx	Tap the Folder icon and then under **File**, select New.

3 From the **Create New Document** dialog box, select a session template.

4 In the **Compatibility** drop-down box, select the set of default settings you want to use for this session, if any.

The compatibility settings include keyboard maps and themes similar to those of other emulation products. The default Reflection compatibility setting is optimized for this product.

5 Click **Create**.

6 For **Host Name/IP Address**, enter the fully qualified host name.

NOTE: Both IPv4 addresses (in the form 127.0.0.1) and IPv6 addresses (in the form 2001:0db8:3c4d:0015:0000:0000:abcd:ef12) are accepted.

---

7 Change other settings if necessary.

8 If you want to add custom files (for example, custom themes, keyboard map, or Ribbon files), select **Configure additional settings** and click **OK**. Then, on the Settings dialog box, click the link for the file you want to customize (for example, Manage Themes, Manage Ribbon, or Manage Keyboard Maps) and follow the online instructions to select a custom file.

9 From the Quick Access Toolbar, click the **Save** button to save the session document.

Open a Terminal Session

To access a host, you need to open a session on that host. Once you've created and saved a session document, you can connect to the host simply by opening the session document.

To open an existing terminal session

1 Go to the Open dialog box.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	From the Quick Access Toolbar, click the **Open** ⬜ button.
TouchUx	Tap the Folder icon and then select ⬜ **Open**.

2 Select the session you want, and then click **Open**.

Connect or Disconnect a Session

To manually disconnect or connect to a session

◆ Do one of the following:

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Session** tab, in the **Host** group, click 🖧 to disconnect or 🖧 to connect.
Reflection Browser	On the **Reflection** menu, choose **Host** and then **Disconnect** or **Connect**.
TouchUx	On the **Reflection** menu, tap the folder icon and then under **Host**, select **Connect**.

Open a Web Session

Reflection includes an integrated browser based on Microsoft Internet Explorer, allowing you to open a Web page in a tab in the Reflection workspace.

To create a Web session document

1 Open the Create New Document dialog box.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	From the Quick Access Toolbar, click the **New Document** 📄 button.
TouchUx	Tap the Folder icon and then under **File**, select 📄 **New**.

2 From the **Create New Document** dialog box, select **Web**, and then click **Create**.

3 From the **Create New Web Session Document** dialog box, under **URL**, type the address of the Web page you want to open.

It is not necessary to type "http://" before the address.

4 Click **OK**.

5 From the **Quick Access** toolbar, click the **Save** button.

The Web page specified will open within the workspace just like a terminal session document, except that the Ribbon will have only one tab. This Ribbon tab shows which application features work within Web pages (Clipboard and Macro), and includes a Navigation group with typical browser controls such as Back and Home buttons.

You can open the same Web page later by clicking the **Open** button on the **Quick Access** toolbar.

Using the Integrated Browser

One of the main benefits of having an integrated browser is the ability to incorporate Web pages into automated tasks. For example, you could create a macro that copies data from an address field in a customer database on the host, then paste that data into a road map Web site such as MapQuest.com, and then display a map to a customer site automatically.

Another key benefit it offers is the automated inclusion of Web sites in your daily workspace. By saving a Web page document with one or more session documents in a Reflection layout, you can instantly create a custom workspace to meet a particular business need. For more information, see the "Create or Modify a Layout" on page 40 topic.

The integrated browser in Reflection is based on Microsoft Internet Explorer, and many of its important features are only accessible through Internet Explorer settings; for example, Internet Explorer security and home page settings affect the Reflection browser.

Get Familiar with the Reflection Interface

With Reflection Desktop, you can display sessions in four types of user interface modes: Ribbon, Browser, TouchUx, and Classic.

In this Topic

Video

▶️ Using the Reflection Ribbon (2:41)

The User Interface Options

The Ribbon

The Ribbon interface shares the look and feel of Microsoft Office. In the area between the Quick Access toolbar (the toolbar in the upper-left corner) and the document window is the Ribbon, a dynamic, collapsible device that organizes commands, buttons, and other controls on tabs for each task area. Double-click any tab in the Ribbon to hide or show the Ribbon. Or, if you prefer, you can map a keyboard shortcut to show or hide the Ribbon with a keystroke.Sessions using the default 3270 or 5250 keyboard map already have this action mapped to CTRL+F1.

The Browser

The Browser interface has a look and feel that is similar to the latest Web browsers. You can access commands from the Reflection menu or from the Quick Access Toolbar. You can also access commands by searching for them in the search box and then clicking on the search results.

TouchUx

The TouchUx interface provides the Reflection TouchUx user experience. Reflection runs on Microsoft Windows devices or other devices (Apple iPad or Android) that are accessing sessions running on a Citrix server. This mode includes an on-screen terminal keyboard that can be set as a transparent overlay or docked in a separate pane.

Classic

A Classic interface option provides an interface that is familiar to users of previous versions of Reflection. When using the Classic UI, only one document can be open in a workspace, and other features may not be available.

Classic MDI

The Classic MDI option is similar to the Classic option. Unlike Classic, it provides a multi-document interface that allows more than one document to be open in a workspace.

To get familiar with Reflection, learn how to navigate and control the ribbon, use the browser, set up keyboard shortcuts, and use other options:

- Select the Interface Type (Ribbon, Browser, Classic, or TouchUx)
- Navigate the Ribbon
- Configure Workspace Arrangement
- Switch Between Tabs and Windows
- Minimize the Ribbon
- Using the Browser
- Use Keyboard shortcuts
- Use Quick Keys
- Switch to Windows Full Screen mode
- Run Sessions Created with other Products

Select the Interface Type (Ribbon, Browser, Classic, or TouchUx)

You can choose from several user interface modes:

- Ribbon shares the look and feel of Microsoft Office.
- Browser has a look and feel that is similar to the latest Web browsers.
- Classic is similar to the Extra! X-treme and legacy Micro Focus Reflection and terminal emulation applications.
- TouchUx provides a touchscreen user experience.

To select the interface type

1 Open the Reflection Workspace Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the File menu or the Reflection button (if using the Office 2007 Look and Feel), choose **Reflection Workspace Settings**.
Reflection Browser	On the Reflection menu, choose **Settings** and then **Reflection Workspace Settings**.
TouchUx	Tap the Gear icon and then select **Reflection Workspace Settings**.

2 Click **Configure User Interface**.

3 In the **User interface mode** list, select the type of interface you want to use.

4 To select a look and feel for the Ribbon or TouchUx interface modes, choose from the options in the **Look and Feel / Color Scheme** list.

5 Close and reopen the workspace.

Navigate the Ribbon

The Ribbon contains tools that you use to complete tasks in the selected document. Tools are represented as button and menu controls, which light up when you select them or move the pointer over them. Related controls are organized into feature groups, such as Productivity and Screen History. Groups are located on tabs, which are organized by function, such as changing the document appearance.
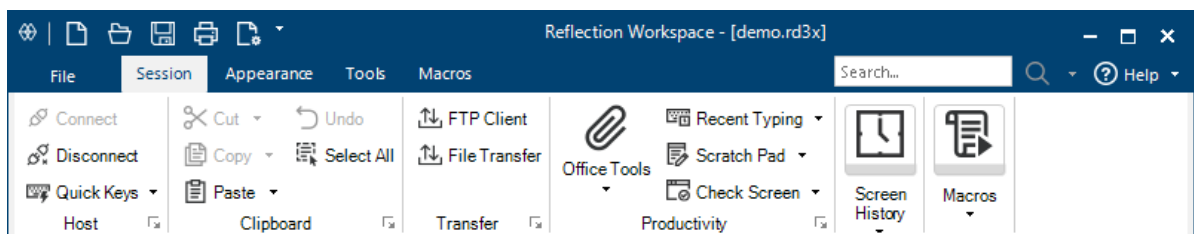
The appearance of the Ribbon and the features available from it depend on the document type and changes you've made to the Ribbon for that document type.

To navigate the ribbon

◆ Do any of the following:

To	Do this
View the entire Ribbon	Expand the workspace by dragging the lower-right corner.
Show or hide the Ribbon	◆ Double-click any tab in the Ribbon. (This method is temporary. The Ribbon is maximized when Reflection is reopened.) ◆ Click **Full Screen** from the **Status bar**. ◆ Map a keyboard shortcut to show or hide the Ribbon with a keystroke. Sessions using the default 3270 or 5250 keyboard map already have this action mapped to CTRL+ F1. ◆ On the Quick Access Toolbar menu, choose **Minimize the Ribbon**.
View a description of a task	Place the pointer over the button.
Open settings for a task	Click the launcher in the lower-right corner of a group.
Go to the next session document or Web page	Press CTRL+ TAB.

To	Do this
Go to the previous session document or Web page	Press CTRL+ SHIFT+ TAB.
Go to the next pane in the current session document	Press CTRL+ 1.
Use your keyboard to interact with the Ribbon	Press ALT to display the KeyTips.

NOTE: You can change the interface appearance from the **Configure User Interface** dialog box. When using the Classic UI, only one document can be open in a workspace, and other features may not be available.

Configure Workspace Arrangement

Reflection provides a variety of ways to customize the appearance of the workspace.

- ◆ Documents in the workspace are displayed in tabs by default. If you are using the Reflection Ribbon, you can choose to display them in windows that can be tiled or cascaded.
- ◆ You can enlarge the document window by using Full Screen mode or by hiding the Ribbon.

To choose tabs or windows

1 Open the Reflection Workspace Setting dialogs box.

   The steps depend on your .

User Interface Mode	Steps
Ribbon	On the File menu or the Reflection button (if using the Office 2007 Look and Feel), choose **Reflection Workspace Settings**.
Reflection Browser	On the Reflection menu, choose **Settings** and then **Reflection Workspace Settings**.
TouchUx	Tap the Gear icon and then select **Reflection Workspace Settings**.

2 Under Workspace Settings, click **Configure User Interface**.

3 In the **Arrange documents as** box, select **Tabs** or **Windows**.

4 (Optional) If you have multiple windows open, you can arrange them as tiled or cascading windows, using the **Arrange Windows** menu, which is next to the **Full Screen** button in the status bar. You can also use this menu to switch the display between tabs and windows.

To enlarge the document window

◆ Do any of the following:

To	Do this
Expand the workspace to fill the entire screen and hide the Ribbon	Click the **Full Screen** button from the status bar; click it again to return the workspace to its normal size and show the Ribbon.
Hide the Ribbon without expanding the workspace	Double-click any tab on the Ribbon; double-click again to show the Ribbon.
Expand the workspace to fill the entire screen without hiding the Ribbon	Double-click the workspace frame in the empty area to the right of the **Quick Access** toolbar; double-click again to return the workspace to its normal size.

Switch Between Tabs and Windows

If you are using the Reflection Ribbon interface and have more than one session document open in a workspace, you can quickly change whether documents are displayed in tabs or in windows.

To quickly switch between a tabbed or windows display

◆ On the right side of the status bar, click the **Arrange Windows** menu and choose whether to display documents in tabs or in cascading or tiled windows.

Minimize the Ribbon

You can minimize the Ribbon to provide more working area in the Reflection window.

To minimize the Ribbon

1 Click the Quick Access Toolbar menu button.

2 In the menu list, choose **Minimize the Ribbon**.

NOTE: You can restore the Ribbon by clicking the Quick Access Toolbar menu button and then choosing **Maximize the Ribbon**.

If you are using a default 3270 or 5250 keyboard map, you can press CTRL+F1 to permanently minimize or restore the Ribbon.

Using the Browser

The Browser interface has a look and feel that is similar to the latest Web browsers. Although it requires less screen real estate than the Ribbon interface, it provides the same functionality as the Ribbon. It also provides additional ways to access commands and connect to hosts.
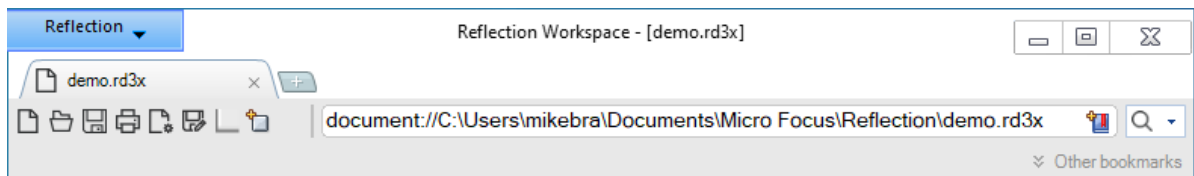
Accessing Commands

In much the same way that you access commands in the Ribbon interface, you can access commands through the Reflection menu or the Quick Access toolbar. The Browser also allows you to access commands by typing them into the search box. For example:

To access the Trace commands, enter `T` in the search box and then choose from the list of Trace commands.

Connecting to Hosts

Similar to the Ribbon, you can connect to a host automatically or from the Reflection menu. In addition, you can connect by entering the type of connection and the host name in the search box.

For example:

To open a telnet connection to a 3270 host named myMainFrame, enter `tn3270://myMainFrame`

NOTE: For IBM systems , you can open Telnet sessions for 3270 or 5250 terminals using the following format:

```
tn3270://hostName
tn5250://hostName
```

For Open Systems (VT) you can open Telnet, Secure Shell, or Rlogin sessions using the following format:

```
telnet://hostName
ssh://hostName
rlogin://hostName
```

Use Keyboard shortcuts

Although it is more common to use a mouse to open dialog boxes, select documents, interact with the Ribbon, and to activate controls, Reflection also allows you to perform these actions using the keyboard.

By creating a custom keyboard map, you can assign a key or key combination to any task or control that you can access from the user interface. You can open a session, run a macro, create an e-mail message, or save a layout. You can also create a sequence of actions to perform with the stroke of a single key.

KeyTips provide another way to access to every command available on the Ribbon or the Quick Access toolbar. You can get to most commands with only two to four keystrokes, no matter where you are in Reflection.

When you press and release the ALTkey, KeyTips are displayed over each feature that is available in the current view. At that point, you can press the letter shown in the KeyTip over the feature that you want to use.

Depending on which letter you pressed, you may be shown additional KeyTips. Continue pressing letters until you press the letter for the specific command or option that you want to use.

Other standard keyboard shortcuts are also supported.

The following table includes common tasks you can perform with the keyboard:

To	Press
Show or hide KeyTips	The ALT key.
Select or use a control on the Ribbon or the **Quick Access** toolbar	ALT,then the key associated with the KeyTip for that control.
Go to the next session document or Web page	CTRL+ TAB.
Go to the previous session document or Web page	CTRL+ SHIFT+ TAB.
Go to the next pane in the current session document	CTRL+ 1.
Move between items in a dialog box	TAB and the ARROW keys.
	-or-
	ALT + the accelerator key (underlined letter) for that item.

Use Quick Keys

Use the Quick Keys gallery on the Ribbon for quick access to terminal keys for host sessions.

To open the quick keys gallery

1 On the Session tab, in the Host group, select the Quick Keys button list.

2 Click the key you want to use. For descriptions of each quick key, see:

   ◆ "3270 Quick Keys" on page 250
   ◆ "5250 Quick Keys" on page 251
   ◆ "VT Quick Keys" on page 252

Switch to Windows Full Screen mode

The Windows Full Screen Look and feel displays the workspace without the standard Windows title bar that includes the minimize, maximize, and close buttons. This Look and feel is available only in the TouchUx User interface mode.

To switch to Windows Full Screen Mode

1 Open the Reflection Workspace Settings dialog box.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the File menu or the Reflection button (if using the Office 2007 Look and Feel), choose **Reflection Workspace Settings**.
Reflection Browser	On the Reflection menu, choose **Settings** and then **Reflection Workspace Settings**.
TouchUx	Tap the Gear icon and then select **Reflection Workspace Settings**.

2 Click **Configure User Interface** to open the User Interface dialog box.

3 In the **User interface mode** list, select **TouchUx**.

4 Select **Windows Full Screen**.

5 Restart the workspace to apply the changes.

Run Sessions Created with other Products

You can run the following types of sessions on Reflection Desktop:

- ◆ Extra!
- ◆ IBM Personal Communications
- ◆ Micro Focus Rumba
- ◆ KEA!

To run one of these sessions, you will need to install the compatibility feature that supports its session files.

NOTE: Extra! and Micro Focus Rumba compatibility features are installed by default.

You will need administrative rights to install this feature.

To install a compatibility feature

1 Open the Reflection Setup program from your administrative installation point or from the Control Panel.

2 On the Feature Selection tab, select **Reflection Workspace** and then **Emulation**.

3 Under **3270/5250** or **UNIX > and OpenVMS**, select **Compatibility**.

4 Choose the compatibility feature for your product and then install the feature.

Cut and Paste

You can copy screen data to the Clipboard and then paste it into other sessions or applications, such as Microsoft Word. You can also configure how text is selected when you copy and paste. From a session in Reflection, you can:

In this Topic

- Use the Clipboard (3270 and 5250)
- Copy and Paste Host Data
- Using a Paste Range
- Undo a Cut or Paste
- Select and Mark Text on a Terminal Screen

Use the Clipboard (3270 and 5250)

In 3270 and 5250 sessions, the Clipboard has a few features that are only available from the Reflection menu: **Paste Next**, **Cut and Append**, **Copy and Append**.

Use **Paste Next** when you have more data in the Clipboard than will fit in a field, and you want to paste the remaining data into another field. Where the **Paste** command would start at the beginning of the data in the Clipboard, **Paste Next** starts at the beginning of the remaining data (that is, the Clipboard contents minus what was pasted in the previous field). Consecutive uses of **Paste Next** gradually empty the Clipboard.

To paste data into multiple fields

1 With data in the Clipboard, place the cursor in the first target field.

2 Select Paste.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	From the **Clipboard** group on the **Session** ribbon, click **Paste**.
Reflection Browser	From the **Reflection** menu, choose **Edit** and then choose **Paste**.
TouchUx	Tap the folder icon and then choose **Paste**.

3 Move the cursor to the next target field.

4 From the Ribbon **Paste** button menu (or the Reflection Browser **Edit** menu), click **Paste Next**.

5 (Optional) Repeat steps 2 and 3 as necessary.

Use **Cut and Append** or **Copy and Append** when you want to add to the Clipboard contents instead of replacing the Clipboard contents.

To append data to the Clipboard contents

1 Select the data you want to add to the Clipboard.

NOTE: You can select a word in a field by double-clicking the word or select all of the words in a field by triple-clicking the field.

2 From the Ribbon **Cut** or **Copy** buttons (or the Reflection Browser **Edit** menu), choose **Cut and Append** or **Copy and Append**.

Copy and Paste Host Data

You can copy entire host screens or selected data to the clipboard, then print the data, paste it to other host screens, Microsoft Office products installed on your computer, or other types of files.

To send host screens or data directly to Microsoft Office products, see "Integrate Host Data with Office Tools" on page 69.

To copy selected data from the current screen to other locations

1 Navigate to the host data you want to copy.

2 Select specific data to copy, then press CTRL+C.

NOTE: You can select a word in a field by double-clicking the word or select all of the words in a field by triple-clicking the field.

3 Navigate to the location where you want to paste the data. This can be on the same host screen, another host screen, or even in another application.

4 Press CTRL+V.

Copy data in a tabular format

You can copy data from the screen and paste it into an application that accepts tabular data (for example, a spreadsheet). By default, table columns are set by analyzing vertical space alignment. Optionally, you can configure Reflection so that columns are set by replacing multiple spaces or tabs with a single tab. (See Configure Clipboard Settings (page 260).)

To copy data from the current screen to a spreadsheet

1 Select the host data to copy.

2 Copy the data as follows:

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the Session ribbon **Clipboard** group, click the **Copy** drop-down menu and then select **Copy Table**.
Reflection Browser	On the **Reflection** menu, choose **Edit** and then **Copy Table**.

3 Open the spreadsheet and press CTRL+V.

To copy host screens from Screen History to another location

1 Open the Screen History task pane.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Session** ribbon, click the ⎘ **Screen History** button.
Reflection Browser	On the **Reflection** menu, choose **View** and then **Screen History.**
TouchUx	Tap the Wrench icon and then under **View**, select ⎘ **Screen History**.

2 Select the screen that you want to copy.

NOTE: Only text areas of the host screen are included in the recorded image; host graphics images are not included.

---

3 From the toolbar in the **Screen History** task pane, click the **Copy** button.

4 Choose **Copy as Text** or **Copy as Bitmap**.

5 Navigate to the location where you want to paste the host screen. This would typically be a file in another application (word-processing, e-mail, and so on).

6 Press CTRL+V.

Using a Paste Range

A paste range defines a region in which you can paste text across multiple screens. After you cut, copy, or append a selection on the Clipboard, you can set the paste range before inserting the selection within the host application. You can also use the Paste Next command to paste text across multiple screens.

NOTE:

The changes you make in the Paste Range dialog box are retained only while your session is open and are not saved when you close your session. If you close and reopen your session, you'll need to adjust these settings again. You cannot save these settings. If you need to define a paste range that you can reuse after you close and reopen your session, you can create a VBA macro that pastes text into a custom paste range (see the `PasteRange` method in the VBA Help).

Paste Range is supported for IBM 3270 and IBM 5250 terminals.

To paste Clipboard information over multiple screens within a host application

1 In a host application or another Windows application, cut, copy, or append a selection on the Clipboard.

2 Open the Paste Range Dialog Box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the Session tab, on the **Paste** drop down menu, select **Paste Range**.
Classic IBM	On the **Edit** menu, select **Paste Range**.

3 Edit the paste range for the **First screen** and **Remaining screens** as needed to fit the paste area.

4 If you need to specify a different page down key to send, select it from the **Page Down** list.

This terminal key is used to scroll automatically to the second and remaining screens of the paste range when the pasted text exceeds the end of the screen.

5 Click **OK** to paste the data into the paste range you specified.

NOTE: For more about Paste Range settings, see "Paste Range Dialog Box" on page 263

Undo a Cut or Paste

You can undo the latest cut or paste you make in an IBM terminal window.

To undo a cut or paste

On the Reflection Ribbon, click ↩.

NOTE

⬦ When you undo a cut or paste, any data you have typed in since that cut or paste is removed.

⬦ After you undo a cut or paste, you can choose to redo it by clicking ↩ again.

Select and Mark Text on a Terminal Screen

Reflection provides two different styles for selecting and marking text on the terminal screen, using either your keyboard or your mouse.

You can select and mark any rectangular area on the screen, or you can select and mark contiguous lines on the screen. You can also set the default behavior for your terminal sessions.

To set the default for selecting text on VT sessions

1 Open the Document Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click 🗋.
TouchUx	Tap the Gear icon and then select 🗋 **Document Settings**.

2 In the Settings dialog box, select **Configure Terminal Settings**.

3 In the Terminal Setup dialog box, select the Keyboard & Mouse tab.

4 To set text selection so that selected text forms a rectangle (instead of wrapping), select **Rectangular selection**.

To set the default for selecting text on IBM sessions

1 Open the Document Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ⬚.
TouchUx	Tap the Gear icon and then select ⬚ **Document Settings**.

2 In the Settings dialog box, select **Configure Terminal Settings**.

3 To set text selection so that selected text forms a rectangle (instead of wrapping), select **Rectangular selection (mouse)**.

To select text using the non-default behavior

◆ (IBM only) When using the mouse, to use the non-default behavior, hold down the CTRL key while dragging the mouse.

-or-

◆ (VT and IBM) When using a keyboard, to change the default behavior, select the **Screen Selection (Keyboard)** action in the Keyboard Mapper, and then choose either **Rectangular Block** or **Contiguous Lines**.

Related Topics

   ◆ "Integrate Host Data with Office Tools" on page 69

   ◆ "Configure Clipboard Settings Dialog Box (3270 and 5250)" on page 257

   ◆ "Clear the Clipboard on Close" on page 250

Capture Screen History

Screen History creates recordings of IBM 3270 and 5250 host screens as you navigate to them.

In this Topic

◆ Capture Screen History

◆ Capture Screens Manually

◆ Navigate Screen History From the Ribbon

Videos

◆ ▶ Using Screen History (1:42)

◆ ▶ Creating Training with Screen History (1:10)

Capture Screen History

Screen History creates recordings of IBM 3270 and 5250 host screens as you navigate to them. VT screens can be recorded using manual capture. You can view and/or verify the information from those screens, and send multiple host screens to Microsoft Word, PowerPoint, and Outlook (Email Message and Note only), if they are installed on your computer.

NOTE: Only text areas of the host screen are included in the recorded image; host graphics images are not included.

To view past screens

1 Open the Screen History task pane.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Session** ribbon, click the ⏱ **Screen History** button.
Reflection Browser	On the **Reflection** menu, choose **View** and then **Screen History.**
TouchUx	Tap the Wrench icon and then under **View**, select ⏱ **Screen History**.

2 Click a screen thumbnail.

   The screen snapshot appears in the main window.

The following commands are also available from the toolbar in the Screen History task pane:

Click	To do this
💾	Save the contents of the Screen History task pane as a file (.RSHX). When you close your session, your screen history is not maintained unless you save it to a separate file. To reopen the file later, it must be saved in a trusted location.
📂	Open a previously saved Screen History file.
📋	Copy the selected screen to the Clipboard as text or a bitmap image.
📎	Open the Office Tools dialog box to send one or more host screens from your screen history to Microsoft Word, PowerPoint, or Outlook (Email Message and Note only), if they are installed on your computer.
⌞O⌟	Create a manual screen capture within the Screen History task pane. (This is helpful for when you want to capture any text you've entered before you leave the screen.)
🗔	Return to the currently active host screen.
A↓Z	Show the most recent screens at the top of the task pane. Click again to revert to the original order.

Click	To do this
	Clear all of the contents at once.
	Put the task pane into auto-hide mode. This collapses the task pane against the side of the application frame. (To re-open the task pane, mouse over the side of the frame.)

Capture Screens Manually

There are two reasons you might want to capture a screen manually: you disabled screen history recording in the **Configure Screen History** dialog box, but need to capture a screen; or you modified one or more unprotected fields in a screen, and want to capture the screen with the modifications.

NOTE: Only text areas of the host screen are included in the recorded image; host graphics images are not included.

To capture a screen manually

+ From the **Screen History** task pane, click the **Manual Capture** toolbar button.

  The current screen, including any data you have entered, is captured and included in your Screen History list.

Navigate Screen History From the Ribbon

You can navigate "Screen History" on page 900 one screen at a time in the main Reflection window directly from the **Session** ribbon without opening the **Screen History** gallery or task pane.

NOTE: Only text areas of the host screen are included in the recorded image; host graphics images are not included.

To navigate screen history

+ Do one of the following:

On the Session ribbon, click	To navigate
The **Back** button	Among captured screens.
The **Forward** button	Forward one screen at a time (if you navigated back, away from the current live screen).
The **Live Screen** button	Directly back to the current, live screen.

Related Topics

+ "Configure Screen History Dialog Box" on page 281

Work with More than One Session

In Reflection, the size, location, and arrangement of the workspace and any open terminal or Web session documents can be saved to a layout file. When opened, a layout automatically opens and arranges all documents saved to the layout, opens and positions any docked panes (such as Scratch Pad or Screen History), and connects session documents to configured hosts.

If the workspace is configured to display documents as tabs, you can create a name for each tab. This can be useful when you use two different applications on one host. You can create a session document that connects to that host, then open the document twice, add a different name to each tab, and then save your layout.

If you are using the Classic user interface mode, you can arrange multiple sessions on your desktop and save them in a layout. The next time you open the layout, you'll find everything in place just the way you left it.

To make it easier to work with more than one session, you can:

In this Topic

- Create or Modify a Layout
- Open a Layout
- Set Tab Colors

Videos

▶️ Creating and Using Layouts (1:52)

▶️ Working with Sessions (1:32)

Create or Modify a Layout

By saving terminal sessions you use regularly to a layout, you can open them all at once, arranged as you prefer, just by opening the layout.

NOTE: If you already have terminal session or Web session document open when you open a layout, the layout opens in a new workspace.

To create a layout

1 Open the documents and any docked panes you want to include in the layout.

2 If you want to be able to access multiple layouts using the Reflection .NET API, enter the necessary API settings as follows:

    2a Open the Layout Settings dialog box.

        The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	
Reflection Browser	On the **Reflection** menu, choose **Settings** and then **Layout Settings**.
TouchUx	Tap the Gear icon and then select **Layout Settings**.
Classic or Classic MDI VT	From the Setup menu, choose **Layout Settings.**
Classic or Classic MDI IBM	From the Options menu, choose **Layout Settings**.

2b Enter the appropriate values for the server and channel name.

3 If the workspace is configured to display documents as tabs, you can add a descriptive label to each document tab:

3a Right-click the session tab, and then choose **Tab Properties**.

3b In the **Name** box, type in the name that you want to appear on the tab, and then click **OK**.

4 Carefully arrange all the session windows until you have set everything up just the way you want it.

  ◆ If you are using the Classic user interface mode, arrange the sessions on your desktop.

  ◆ For other interface modes, arrange the windows in the workspace and adjust the size and position of the workspace, as needed.

5 Save the layout.

The steps depend on your .

User Interface Mode	Steps
Ribbon	
Reflection Browser	On the Reflection menu, choose **Save Layout**.
TouchUx	Tap the Folder icon and then select **Save Layout**.
Classic or Classic MDI VT	From the File menu, choose **Layout**. and then **Save Layout As.**
Classic or Classic MDI IBM	From the File menu, choose **Save Layout**.

6 Name and save the layout file to a trusted location, and then click **Save**.

If you haven't saved the session documents, you are prompted to do so.

To modify a saved layout

  ◆ To save changes to a layout, save it again using the same name.

NOTE: Reflection doesn't prompt you to save changes to a layout.

Open a Layout

By saving terminal sessions you use regularly to a layout, you can open them all at once, arranged as you prefer, just by opening the layout.

NOTE: If you already have terminal session or Web session documents open when you open a layout, the layout opens in a new workspace.

To open a layout

1 Go to the Open dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	From the Quick Access Toolbar, click the **Open** button.
TouchUx	Tap the Folder icon and then select **Open**.
Classic or Classic MDI	From the File menu, choose **Open**.

2 Select the layout file you want, and then click **Open**.

Layout files created in Reflection end with the extension `.rwsp`.

Set Tab Colors

When you are running multiple sessions, color-coding session tabs can help identify which host application each session is connected to.

You can customize the text and background colors of a session tab. After you set the tab colors for your sessions, you can save them in a layout file so that the tab colors are used the next time you open the layout.

NOTE

- You can save session tab color settings only in layout files. These settings are not saved in session files.
- You can change only one tab at a time. You cannot globally change all tab colors.

To set tab background and text colors

You can set different colors for a session tab's text and background. You can also set different colors for active and inactive states.

1 On the Session tab, right-click and then select **Customize Tab Colors** to open the Customize Tab Colors dialog box.

2 To set inactive tab colors, in the **Inactive tab colors** list, click **Change** and then select the foreground (text) color or background color.

3 Set the Active tab colors in the same way.

4 Save the color settings in a layout.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **File** menu or the Reflection button ⏣ (if using the Office 2007 Look and Feel), choose **Save Layout**.
Reflection Browser	On the Reflection menu, choose **Save Layout**.
TouchUx	Tap the Folder icon and then select **Save Layout**.

TIP: If you want to set only the tab background color, you can use an alternative approach. With a session open, click the **Appearance** tab and from the **Color** menu, choose a color. Then click on the session tab to set its background color. (The selected color is used as the tab's background, for both active and inactive states.)

Related Topics

Moving from Extra! to Reflection

If you're moving from Extra! to Reflection, you'll find that some things are very similar, while others are different or new to you. This article shows Extra! users how to customize terminal sessions in Reflection. It shows how to find the settings you want to configure, points out differences between how some of the settings work, and shows what's new for Extra! users.

Opening Extra! Sessions in Reflection Desktop

You can open Extra! (`.edp`) session files in Reflection Desktop to automatically convert them to Reflection Desktop sessions. When you save these files, they are automatically converted to the new Reflection Desktop session file format. Many of the supporting files referenced by the sessions you

open (keyboard and mouse maps, QuickPads, toolbars, and Hotspots) are also converted when you save the sessions. For a list of supported files, see Supported Extra! Files in the Reflection Deployment Guide.

NOTE

- In addition to `.edp` files and their associated support files, you can also open Ind$File file transfer session files.

- You cannot open `.epp` files and most file transfer sessions.

- Only Hotspot text mappings are imported. Region mappings are not imported.

To open Extra! session files along with supporting files

1 If you use a user data directory or Extra! directory other than the default (under `...Users\user\Documents\Micro Focus\)`, make sure the session files are in trusted locations.

   NOTE: When the Trusted Locations security feature is enabled, Reflection does not allow you to open files unless they are in trusted locations. For information about trusted locations and how to configure them, see "Specify Trusted Locations Dialog Box" on page 426.

2 From the Reflection Desktop File menu, open the `.edp` session file.

3 Verify that all of your custom settings, such as toolbars, QuickPads, keyboard maps, and other custom settings work as expected.

4 If Reflection is not using all of your customized settings, make sure these files are in the same location as the session (`.edp`) file.

   NOTE: If Reflection cannot find custom settings files, it uses default settings.

5 Save the session file in the **Default user data** directory specified in **Configure workspace attributes**.

   - If you want to use the supporting files you imported for other sessions, choose **Save** from the **File** menu. All of the settings and supporting files referenced by the session are saved under the user data folder. These files are automatically converted to the new Reflection file formats.

   - If you are deploying the file to a centralized environment (such as Citrix), consider saving the file as a compound session document. This saves all of the supporting settings in a single file.
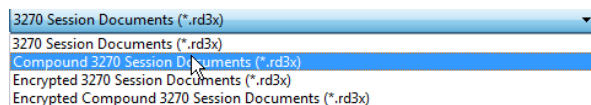
Creating a Session

Creating sessions in Reflection is somewhat different from the process you used for Extra! Instead of using a wizard that walks you through configuration settings, you'll select from a set of templates to create the type of session you want and then configure settings for that session in a settings dialog box.

To create a Reflection Desktop session

1 On the toolbar (or the Quick Access toolbar), click ▯ to open the Create New Document dialog box.
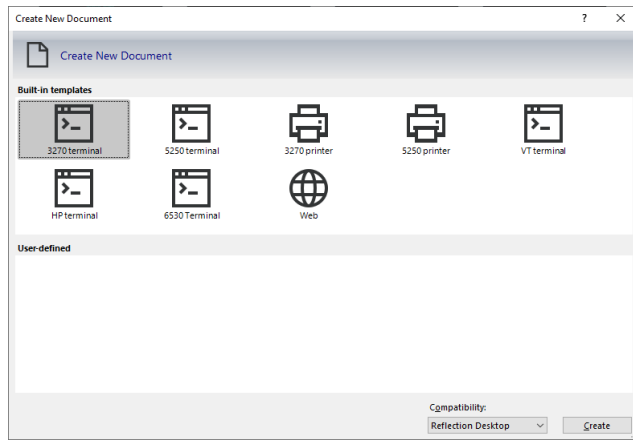
2 If you are creating an Extra! VT terminal session, choose the **Extra!** option in the **Compatibility** list.

NOTE: This setting specifies which built-in keyboard maps, themes, Hotspots, and other settings to use for the session. You don't need to change this for IBM terminal sessions, because the default Reflection Desktop option uses Extra! settings for those sessions.

---

3 Choose the type of session to create and then click **Create**.

4 In the Terminal Document Settings window, enter the **Host name**, **Port** and other connection settings for the session.

5 To set up additional settings, select **Configure additional settings**.

The Reflection Settings Window that you will use to configure and manage your session settings is displayed.

Using the Reflection Settings Window

Most of the utilities and configuration options in the Extra! Settings window can be accessed and configured from the Reflection Settings window.

If you are using the Reflection Classic user interface mode (which is very similar to the Extra! user interface), you can open this window in the same way you do in Extra!, by selecting **Settings** from the **Options** menu.

While the Reflection Settings window includes most of the items in the Extra! Settings window, there are a few important differences.

Organization

The items in the Reflection Settings window are organized a little differently than in Extra!'. It's appearance is flatter and some of the items are found in different groups. Some of the items also have different names.
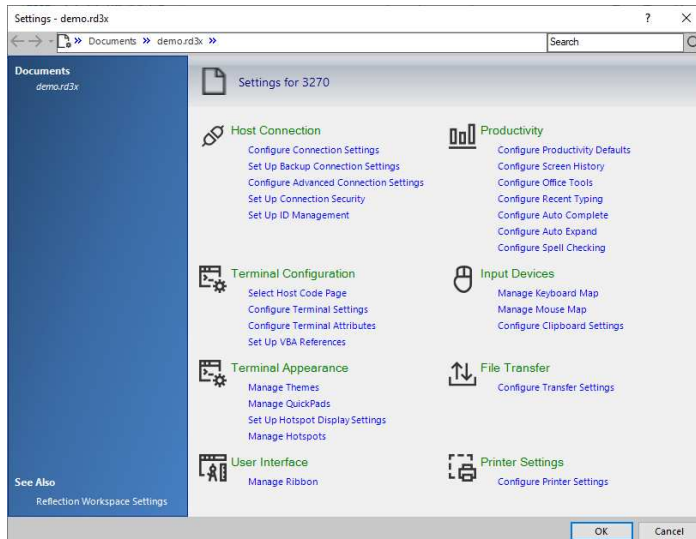
Navigation

After you select an item to configure, you'll navigate the Settings window differently than you did in Extra!:

  • Instead of using high level links to all the items on the left pane, you'll use **Jump To** links to jump to other areas of the dialog box you have opened and **See Also** links to go to other dialog boxes in this group.

  • You can use the breadcrumbs at the top of the window to go to different groups.

  • You can use the Back button just as you would a Back button in a Web browser.

  • If you are having a hard time finding a setting, use the Search.

Connection Settings

The Extra! Connection category settings are found in several Reflection dialog boxes that can be accessed under the Host Connection group in the Settings window.

To find these Extra! Settings	In the **Host Connection** group, select…
Basic non-security related connection settings (IP address, port, etc.) available in the Extra! Configure Connection dialog box	**Configure Connection Settings**.
The security settings in the Extra! Configure Connection dialog box	**Set up Connection Security** to open the Reflection Security Properties dialog box.
	If you set up a SSL/TLS connection, select **Configure PKI** for settings related to certificates.
Extra! Connection categories **Advanced** tab settings	**Configure Advanced Connection Settings**
ID Management options.	**Set up ID Management**

For more, see:

- Connect to Hosts and the Web
- Set up Sessions and Connections

Display, Colors, and Fonts Categories

Display options for cursor appearance are configured along with fonts and colors in Reflection files called themes. Each session file is associated with a theme.

NOTE: Additional settings similar to Extra! **Text display options** and **Graphics display options** are configured in the Configure Connection Settings dialog box, accessed from the Reflection Settings window.

When you open and save an Extra! session, the session and an associated theme are saved in Reflection file formats. The new theme file has the same name as the session file and is associated with the new session file.

You can modify any of the theme settings by modifying an existing theme or by creating a new theme from an existing theme. If you want to associate a new theme with a session after your theme is configured, you'll need to apply the theme to the session.

To configure a theme

1 In the Settings window, under the **Terminal Appearance** group, select **Manage Themes**.

2 In the Manage Themes dialog box, select **Modify the currently selected theme** or **Create a new theme from an existing file**.

3 If you are creating a new theme, choose a theme to base your theme on.

NOTE: If you want to automatically associate the new theme with your session, make sure **Use the new file in the current session document is selected**. Alternatively, you can select to associate the theme with the current session after you configure it.

---

4 In the Modify Theme dialog box, set the colors, fonts, and cursor display options for your theme and save the theme.

Theme files are saved as `.themex` files in the `Themes` folder in your user data directory.

For more, see:

◆ Change the Look and Feel of a Session

Edit Category Settings

Extra!'s Edit category settings are found in the Reflection Desktop Configure Clipboard Settings dialog box.

To access Edit category settings in Reflection Desktop

1 In the Settings window, under the **Input Devices** group, select **Configure Clipboard Settings**.
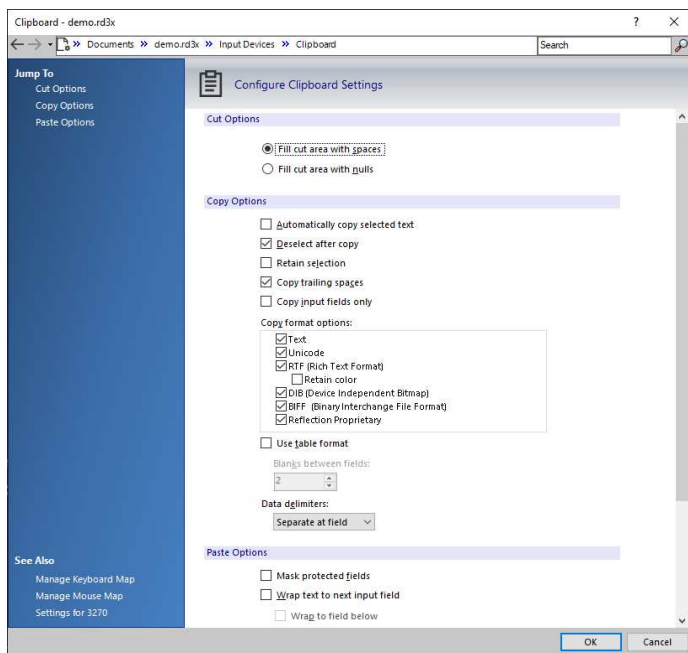
The settings you configure are saved in your session file.

For more, see:

◆ Configure Clipboard Settings Dialog Box (3270 and 5250)

Hotspots

When you open and save an Extra! session that is associated with a Hotspot file, the session and the Hotspot are saved in Reflection file formats. The new Hotspot file has the same name as the session file and is associated with the new session file.

NOTE: Only Text Hotspots mappings are imported. Region Hotspots mappings are not imported. Modifications to `.ehs` Hotspots files are saved using the Reflection Hotspots file format and extension (`*.xhs`).

You can modify Hotspots by selecting **Manage HotSpots** in the Settings window and then choosing whether to create a new Hotspot or modify your existing Hotspot. The Hotspot editor is very similar to the Extra! editor.
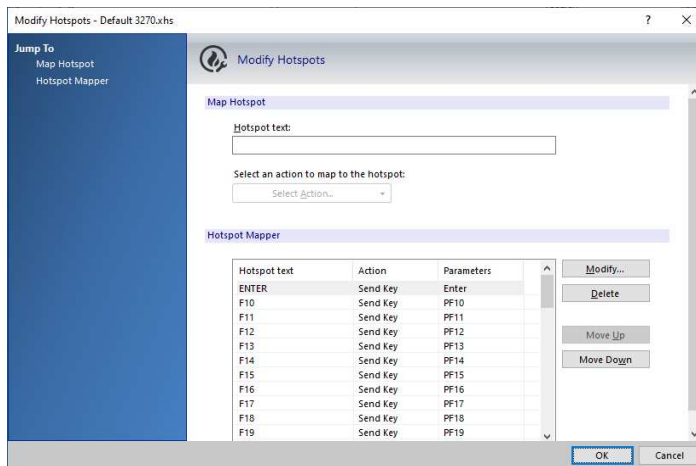
You can also import Hotspots that are not associated with a session file and convert them to the new format.

To convert a Hotspot file

1 Place the Hotspot file in the `My Documents\Reflection\Hotspots` Maps folder.

2 In the Settings window, select **Manage Hotspots**.

3 Choose **Select another Hotspots file**.

4 Select **Custom**, and browse to the file.

5 Select to **Modify the currently selected Hotspots file** and then save it in the new file format (`.xhs`).

For more, see:

◆ Set up Custom Controls for your Program Screens

Keyboard Maps

When you open and save an Extra! session that is associated with a keyboard map file, the session and keyboard map are saved in Reflection file formats. The new keyboard map file has the same name as the session file and is associated with the new session file.

You can open the keyboard mapper from the Settings window by choosing **Manage Keyboard Maps** under **Input Devices** and selecting whether to create a new map or modify an existing one.
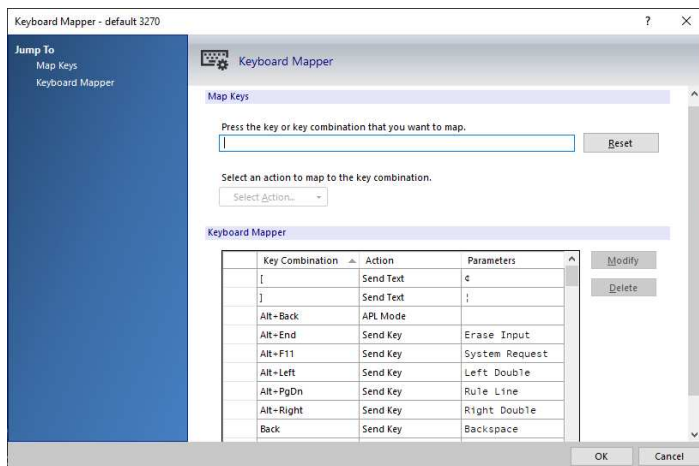
The Reflection keyboard mapper works a little differently than the Extra! mapper. Instead of displaying a graphical map that you interact with, the Reflection mapper provides a table that includes all the keys and their values.

To map a new key action

1 In the Settings window, under **Input Devices**, select **Manage Keyboard Map**.

2 Enter the key or key combination and then click the **Select Action** button.
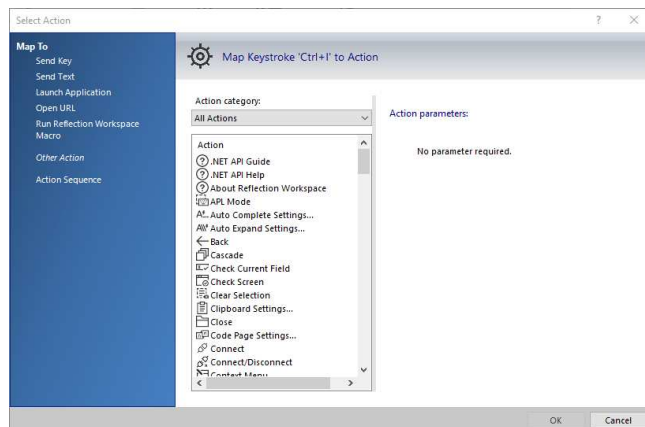
3 In the Select Action box, choose the action to associate with the key.

To modify a key action

1 Select the key in the table and then click **Modify**.

2 In the Select Action dialog box, choose the action to map the key to.

NOTE: You can also create new keyboard maps or new mouse maps. If you want to automatically associate a new map with your session, make sure **Use the new file in the current session document is selected**. Alternatively, you can select to associate the map from the Manage Keyboard Map or the Manage Mouse Map dialog box after you configure it.

For more, see:

◆ Select and Map the Keyboard and Mouse

Menus and Toolbars

You'll use the same process to create menus and toolbars as you used in Extra! but you'll find that the UI Designer is a little different from Extra!.

To create or edit menus or toolbars

1 In the Settings window, under **User Interface**, select **Manage Ribbon**.

NOTE: Although the Reflection interface references the Ribbon throughout this process, it applies to toolbars and menus if Reflection is in Classic mode.

---

2 Select whether to **Modify the currently selected Ribbon file** or **Create a new Ribbon from an existing Ribbon file**.

3 If you are creating a new file, browse to a file to use as a template.

4 If you want to associate a new menu or toolbar with the current session, select **Use the new file in the current session document**.

NOTE: Alternatively, you can select to associate the menu or toolbar from the Manage Ribbon dialog box after you configure it.

When Reflection is in Classic mode, the UI Designer displays an interface you can use to modify toolbars and menus, as shown below.
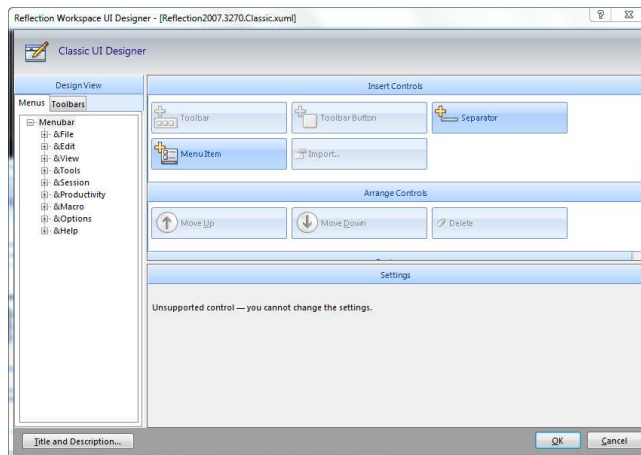
When Reflection is in Ribbon interface mode, the UI Designer displays an interface that can be used to modify the ribbon.

Productivity

Configuring productivity settings such as Spelling, Auto Complete, Auto Expand and Recent Typing is very similar to Extra!.

Instead of tabs, these options are displayed in dialog boxes that are accessed under the Productivity group in the Settings window.

Most of the settings on the Productivity General tab are found by selecting Configure Productivity Defaults.
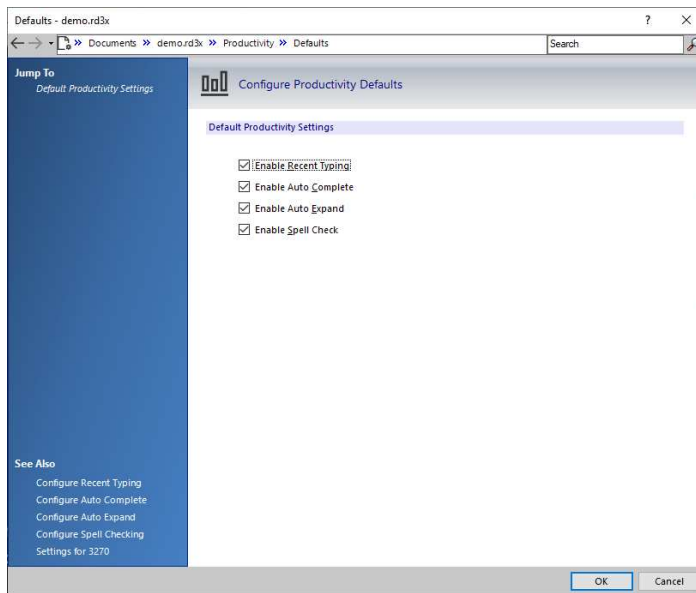
NOTE

- Screen History is disabled by selecting **Manual capture only** on the Configure Screen History dialog box.
- Office Tools and enable Scratch pad are always on.

For more, see:

- Set up Productivity Features

QuickPads

You can use Extra! QuickPads in Reflection. If you are deploying QuickPads, it's a good practice to save them in the new Reflection QuickPad file format (`.rqpx`). You can do this by selecting to modify the QuickPads.

Editing QuickPads in Reflection is similar to how you edit them in Extra!.

To create or modify a QuickPad

1 On the Settings window, under **Terminal Appearance,** select **Manage QuickPads**.
2 Select whether to modify a QuickPad or create a new one.

The new QuickPad editor has been redesigned to provide a more modern graphical layout for designing QuickPads.
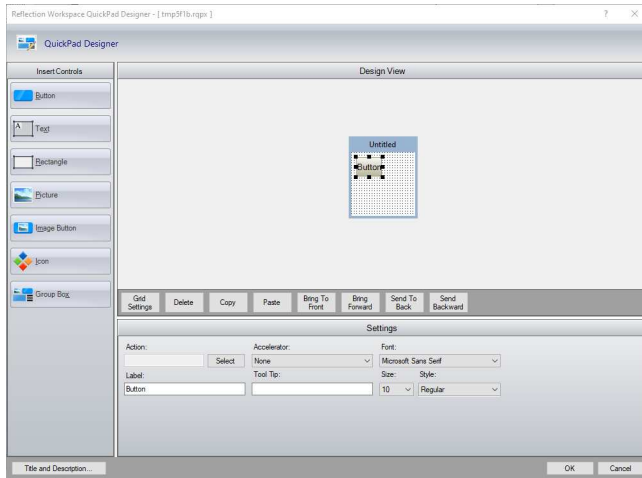
3 How Do I?

The following articles and videos show some how to customize and configure Reflection.

In This Section

- Set up Sessions and Connections to automatically connect, use session templates, encrypt session files, and start sessions from the command line.

- Select and Map the Keyboard and Mouse to create keyboard and mouse maps and shortcuts, and select a custom map for a session.

- Set up Productivity Features such as Auto Complete, Auto Expand, Spell Check, Scratch Pad, Recent Typing, and Screen History to accelerate data entry and host navigation, maximizing user productivity, while reducing errors.

- Change the Look and Feel of a Session including color settings, cursor styles, sounds, underlining of input fields, and which dialog opens when Reflection starts. Control these options and more by creating and using custom theme files.

- Set up Custom Controls for your Program Screens to provide a modern interface with new features and capabilities. You can also enhance your program interface using Reflection Hotspots (virtual buttons that appear over text in terminal sessions).

- Record, Run, and Edit VBA Macros created in Reflection, and most macros created with Extra! and legacy Reflection products. You can also run the majority of macros created with the Micro Focus Rumba, IBM Personal Communications, OpenText HostExplorer, and Brandon Systems\Jolly Giant QWS3270 products.

- Set up Actions for Reflection Events to initiate Reflection actions, such as Reflection macros, and menu and terminal commands when an event is encountered during a host session. This makes it possible to monitor Reflection/host interactions and synchronize Reflection commands with a defined group of host session events.

- Customize the Ribbon to add or remove, or modify ribbon controls, import legacy toolbars, change the Quick Access Toolbar, and minimize the ribbon.

- Customize Classic Menus and Toolbars used by your Reflection Desktop sessions. You can set up sessions to share the same customized menus and toolbars or you can set up unique menus and toolbars for each session. You can also import toolbars from Reflection 14 or Extra! sessions and then save them in Reflection .xuml files that can be applied to other sessions.

- Set up Workspace Settings that apply to all sessions, including: accessing a Centralized Management Server that you have set up to centrally manage and control sessions, performing a series of actions when the workspace starts, and saving sessions as compound session document files that contain session settings in a single file.

- Perform Other Common Tasks such as broadcasting commands to multiple VT sessions, capturing incoming screen data or sending special character data on VT sessions, using customized host files, editing the translation table, and generating a HLLAPI trace.

- Print a list of screens and then specify how many screens to print on a page or set up Reflection to print multiple screens as a continuous flow of text, without page breaks at the beginning or end of screens.
- Transfer Files to IBM mainframes HP3000, UNIX, and VMS Systems, transfer files with FTP, and configure non-FTP file transfer.

Videos

- ▶ Working with Sessions(1:32)
- ▶ Map a Keyboard in Reflection Desktop (2:41)
- ▶ Using Productivity Features (2:28)
- ▶ Changing a Session's Look and Feel (1:10)
- ▶ How to Record a Macro When Using the Reflection Desktop Classic Interface(2:31)
- ▶ How to Record a Macro When Using the Reflection Desktop Ribbon(1:14)
- ▶ Running Extra! Macros Reflection Desktop (3:06)
- ▶ Using the Reflection Ribbon(2:48)
- ▶ Customizing the Ribbon (3:04)
- ▶ Using the Quick Access Toolbar (1:12)
- ▶ How To Customize Menus and Toolbars in Reflection Desktop Classic Mode (3:40)

Set up Sessions and Connections

Using options for starting and configuring Reflection, you can automatically connect, use session templates, encrypt session files, and start sessions from the command line.

In this Topic

- Specify Whether to Automatically Connect to the Host
- Share Sessions as Templates
- Encrypt a Session File
- Start a Session From a Command Line
- Configure Host Connection Options

Video

▶ Working with Sessions(1:32)

Specify Whether to Automatically Connect to the Host

By default, terminal session documents are configured to connect to the host automatically when you create or open a terminal session. However, with a session document open in Reflection, you can manually disconnect or connect. You can also set up a session so that it doesn't automatically connect to the host.

To stop a session from automatically connecting to the host

1 Open a terminal session.

2 Open the Document Settings dialog box.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ![icon].
TouchUx	Tap the Gear icon and then select ![icon] **Document Settings**.

3 Under **Host Connection**, click **Configure Connection Settings**.

4 Under **Host Connection Options**, clear the **Automatically connect to the host** option.

Share Sessions as Templates

Session documents contain references to the following settings (all of which can be customized): host, ribbon, theme, keyboard map, and mouse map.

After you configure a session document, you can share and reuse your settings by saving the document as a template. Templates provide an untitled copy of the original, giving you a quick and easy way to create pre-configured documents, while ensuring that your original file remains unchanged.

Reflection includes several templates in the **Create New Document** dialog box. When you create a template, as long as you save it to the Templates folder (the default location), it is added to this dialog box under **User Defined**.

To share a session document

1 Open the session document that you've configured.

2 Save the session as a template.

   2a Do one of the following:

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **File** menu or the Reflection button ![icon], choose **Save As** and then **Save Template.**
Reflection Browser	In the search box, enter `S` and then, under **Actions**, select ![icon] **Save Template**.

   2b Name the template file with an .rsft extension, and then save the template to the Templates folder.

3 Move the template file from the Templates folder on your computer to either a shared location or to the Templates folder on a computer that has Reflection installed.

NOTE: If you copy the template file to a location other that the Templates folder, make sure it's a trusted location or Reflection won't open it.

The Templates folder is in the following location:

```
Users\ user_name\AppData\Roaming\Micro Focus\Reflection\Desktop\version
\templates
```

4 To make changes to the template, you must replace the template file — save the file that contains your changes using the same filename and extension as the template.

Encrypt a Session File

You can encrypt 3270, 5250, and Open Systems session documents to protect them against unauthorized changes. Encryption effectively scrambles the data in a session document, helping to prevent unauthorized users from reading and changing the file's contents. For best results, use document encryption in conjunction with the encryption options in the Permissions Manager.

In Reflection, you can easily encrypt sessions by saving them in the Encrypted Session Document format.

Alternatively, you can encrypt documents using a command-line program installed with Reflection, `FileEncrypt.exe`. With this program, you can also determine whether session documents are encrypted, and if they are, you can decrypt them.

To encrypt a session in Reflection

1 Open a session document.

2 Open the **Save As** dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the File menu or the Reflection button ⚙ (if using the Office 2007 Look and Feel), choose **Save As**.
Reflection Browser	On the **Reflection** menu, choose **Save As**.
TouchUx	On the **Reflection** menu, tap the Folder icon and then under **File**, select **Save As**.

3 From the **Save as Type** list, choose the available encryption format, and then click **Save**.

To encrypt, decrypt, or test sessions using FileEncrypt.exe

◆ From a command line, enter any of the following commands:

To	Type
Encrypt a document	`fileencrypt /e` [*file_in*] [*file_out*]
Decrypt a document	`fileencrypt /d` [*file_in*] [*file_out*]
Test a document for encryption	`fileencrypt /t` [*file_in*]

where:

[*file_in*] =The filename, including the extension and relative path.

[*file_out*] =(Optional) A new name for the output file.

For example:

`fileencrypt /e Session.rd3x SessionEncrypted.rd3x`

NOTE: `FileEncrypt.exe` searches only the current directory for session files, and requires administrative credentials to encrypt or decrypt a file.

Start a Session From a Command Line

You can launch a Reflection session from a command line. You can also use command line options to specify Reflection startup behavior and appearance. These options override the workspace settings.

To start a session

◆ On a Windows command prompt, enter the following commands:

`"Attachmate.Emulation.Frame.exe" -f "<sessionPath><sessionName>"`

Reflection Command Line Options

Options are case insensitive and are preceded by either a dash (-) or forward slash (/).

-f

Open document (. `rdox`, . `rd3x`, . `rd5x`) or layout (. `rwsp`)

-n

Suppress Reflection splash screen

-uimode{classic|ribbon|browser|touch}

Set user interface mode

-?, -help

Display this help topic

For example:

The following command opens `mysession.rd3x` in Browser mode with the splash screen suppressed:

```
Attachmate.Emulation.Frame.exe -f "C:\Users\myUserName\Documents\Micro
Focus\Reflection\mysession.rd3x" -uimode browser -N
```

Configure Host Connection Options

You can specify whether to automatically connect to the host when a session document is opened. You can also specify whether to reconnect to a host after disconnections occur that are not initiated from Reflection.

To set up Host connection options

1 Open the Document Settings dialog box.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click .
TouchUx	Tap the Gear icon and then select **Document Settings**.

2 Under **Host Connection**, click **Configure Connection Settings**.

3 Under **Host Connection Options** (or **Connection Options** if you are using VT), specify how to connect and what to do when a connection is terminated:

   ◆ To set up the session to establish a host connection as soon as the associated session document is opened, select **Automatically connect to the host**.

   ◆ To specify whether to reconnect after any disconnection that is not initiated from Reflection, select an option in the **When connection is terminated** list.

Select and Map the Keyboard and Mouse

A keyboard map lists host terminal keys and their definitions, as well as all defined keystrokes (shortcuts).

Keyboard map files control the action of keys on your PC keyboard, so that they correspond to specific host keys or provide keyboard shortcuts. When you create a terminal session document, it includes a pointer to a default, built-in keyboard map file. You can choose a different keyboard map file for each session, and you can create custom keyboard map files with the settings you prefer.

You can also set up and select custom mouse maps. When you configure keyboard and mouse maps for sessions, you can:

In this Topic

◆ Use the Graphical Terminal Keyboard

- Select the Keyboard Map for a Session

- Create a Custom Keyboard Map

- Add a Keyboard Shortcut

- Delete a Keyboard Shortcut

- Restore the Default Keyboard Map

- Select the Mouse Map for a Session

- Add a Mouse Action

- Delete a Mouse Action

- Restore the Default Mouse Map

Video

▶️ Map a Keyboard in Reflection Desktop (2:41)

Use the Graphical Terminal Keyboard

You can display a graphical terminal keyboard that allows you to use your mouse or touch screen to enter data or use special keys in your IBM or Open Systems sessions. You can choose from several prebuilt keyboards.
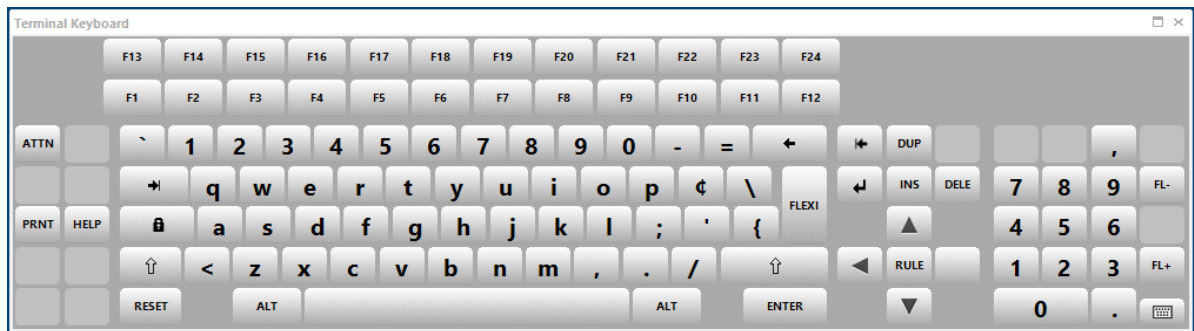
NOTE: you can select different prebuilt keyboards but you cannot change the mappings for each keyboard. If you are using the five supported languages (English, French, German, Spanish, and Japanese), the keyboard displays in the language for your operating system. If you are using an unsupported language, the keyboard displays in English.

To use the graphical terminal keyboard

1 Open a session in Reflection.

2 Display a graphical terminal keyboard as follows:

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the Appearance tab, click **Terminal Keyboard**.
TouchUx	Tap the Wrench icon and then select **Terminal Keyboard**.
Reflection Browser	On the Reflection menu, choose **Tools** and then **Terminal Keyboard**.
Classic	On the session default toolbar, click .

3 To switch keyboards, click in the lower right hand corner of the keyboard.

4 To close the keyboard, select the same terminal keyboard menu item or icon you used to open it.

5 To dock the keyboard to the workspace, select the keyboard title bar and move the cross-hairs to one of the upper, lower, left or right arrows displayed above the keyboard.

The following example docks the keyboard to the top of the workspace.

6 Save the session. When you reopen the session, the keyboard is displayed just as it was when you saved the session.

Select the Keyboard Map for a Session

Reflection pre-configures all session documents to use a built-in keyboard map file. You can choose to use a different built-in map, or a custom map that you've created.

To select a keyboard map

1 Open the Document Settings dialog box.

The steps depend on your .

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ⬚.
TouchUx	Tap the Gear icon and then select ⬚ **Document Settings**.

2 Under **Input Devices**, click **Manage Keyboard Map**.

3 Click **Select another keyboard map file**.

4 Do one of the following:

To	Do this
Select a built-in keyboard map	Click **Built-in**, and then select a map from the list; for example, `Default 5250 en.xkb`.
Select a custom keyboard map	Click **Custom**, and then browse to a custom keyboard map file. **NOTE:** The file must be in a trusted location.

Create a Custom Keyboard Map

Host terminal and PC keyboards have different sets of keys; for example, many terminal keyboards have a Transmit key, but PC keyboards do not. Reflection pre-configures each session document with a built-in "keyboard map" substituting a PC key (or combination of keys) for the terminal function, so that a PC can communicate with a host in the same way as a terminal. You can create a custom keyboard map by adding, removing, or redefining keystroke combinations from an existing keyboard map.

To create a custom keyboard map

1 Open the Document Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ⬚.
TouchUx	Tap the Gear icon and then select ⬚ **Document Settings**.

2 In the Settings dialog box, under **Input Devices**, click **Manage Keyboard Map.**

3 In the Manage Keyboard Map dialog box, click **Create a new keyboard map from an existing keyboard map file**.

4 In the Create a New Keyboard Map file dialog box, select a keyboard map file to use as a template for your new file (for example, `Default 3270.xkb`).

5 If you want to use the new keyboard map file in your current session, choose **Use the new file in the current session document**.

6 Click **OK**.

7 Do one of the following:

To	Do this
Add a keystroke definition	Under **Map Key**s, enter a key combination (keystroke) in the box, click the **Select Actio**n menu, and then choose **Send Key**.
	From the **Key** drop-down box, choose the host terminal key to which you want to map, and then click **OK**.
Change the definition of a keystroke	Select the key combination you want to change and click **Modify**.
	Specify an action for the keystroke, and then click **OK**.
Remove a keystroke definition	Select the key combination you want to remove, and then click **Delete**.

8 When you are done making changes, click **OK**.

9 When prompted, save the new keyboard map in the `Keyboard Maps` folder.

10 If you are prompted that this is not a secure location, click **Yes**.

The file is saved in your `Documents\Micro Focus\Reflection\Keyboard Maps` folder.

Add a Keyboard Shortcut

You can create keyboard shortcuts that perform any assignable action during a Reflection session. For example, using the **Keyboard Mapper,** you can select a standard action, such as **Send Text** or **Launch Application**, or you can create a macro or complex sequence of actions that you assign to a keystroke.

To add a keyboard shortcut

1 Open the Keyboard Mapper Dialog Box.

   1a Open a session in Reflection.

   1b Open the Reflection **Keyboard Mapper** dialog box as follows:

     The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Tools** tab, click **Keyboard Mapper.**
Reflection Browser	On the **Reflection** menu, choose **Tools**, and then **Keyboard Mapper.**
TouchUx	Tap the Wrench icon and then under **Tools**, select **Keyboard Mapper.**

2 Under **Map Keys**, enter a keystroke (for example, CTRL+K).

NOTE: Avoid using keystrokes already defined in the keyboard map.

3 Assign an action by doing one of the following:

- ◆ From the **Select Action** menu, choose a task (for example, **Launch Application**).

  -or-

- ◆ Click the **Select Action** button, and from the **Select Action** dialog box, specify an action or action sequence.

4 Enter parameters for the action, if required, and then click **OK**.

5 Save your changes to a custom keyboard map file.

The new keyboard shortcut appears in the table under **Keyboard Mapper**.

Delete a Keyboard Shortcut

1 Open the Keyboard Mapper Dialog Box.

1a Open a session in Reflection.

1b Open the Reflection **Keyboard Mapper** dialog box as follows:

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Tools** tab, click **Keyboard Mapper.**
Reflection Browser	On the **Reflection** menu, choose **Tools**, and then **Keyboard Mapper.**
TouchUx	Tap the Wrench icon and then under **Tools**, select **Keyboard Mapper.**

2 From the **Keyboard Mapper** table, select the key combination you want to remove.

3 Click **Delete**, and then click **OK**.

4 Save your changes, as needed.

Restore the Default Keyboard Map

If you have problems using a customized keyboard map in a session document, you can restore the default keyboard map.

To restore a default keyboard map

1 Open the Document Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ⬚.
TouchUx	Tap the Gear icon and then select ⬚ **Document Settings**.

2 Under **Input Devices**, click **Manage Keyboard Map.**

3 Click **Select another keyboard map file**.

4 Click **Built-in**, and select a map from the list that matches your host session; for example, for a 5250 host session, choose Default 5250 en.xkb.

5 Click **OK**.

Select the Mouse Map for a Session

A mouse map is a configuration file that shows all of the defined mouse actions and mouse/key combinations for your mouse. Reflection pre-configures all session documents to use a built-in mouse map file. You can choose to use a different built-in map, or a custom map that you've created.

To select a mouse map

1 Open the Document Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ⬛.
TouchUx	Tap the Gear icon and then select ⬛ **Document Settings**.

2 Under **Input Devices**, click **Manage Mouse Map**.

3 Click **Select another mouse map file**.

4 From the **Select a Mouse Map File** dialog box, do one of the following:

To	Do this
Select a built-in mouse map	Click **Built-in**, and then select a map from the list; for example, `mouse.xmm`.
Select a custom mouse map	Click **Custom**, and then browse to a custom mouse map file. **NOTE:** The file must be in a trusted location.

Add a Mouse Action

Using the **Mouse Mapper**, you can assign an action to a mouse click, a wheel up/down, or, to a mouse click and keystroke combination. Each time you perform that mouse action in Reflection, the specified action occurs.

To add a mouse action

1 Open a session in Reflection.

2 Open the Mouse Mapper Dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Tools** tab, click **Mouse Mapper**.
Reflection Browser	On the **Reflection** menu, choose **Tools**, and then **Mouse Mapper**.
TouchUx	Tap the Gear icon and then select **Document Settings**. Under **Input Devices**, click **Manage Mouse Map**. Then choose whether to modify the current mouse map or create a new map.

3 Under **Mouse Mapper**, place your pointer over the image, and then do either of the following:

- ◆ Click a mouse button or wheel up/down.

  -or-

- ◆ Click a mouse button while pressing a modifier key (for example, CTRL).

4 Assign an action by doing one of the following:

- ◆ From the **Select Action** menu, choose a task (for example, **Launch Application**).

  -or-

- ◆ Click the **Select Action** button, and from the **Select Action** dialog box, specify an action or action sequence.

5 Enter parameters for the action, if required, and then click **OK**.

6 Save your changes to a custom mouse map file, if necessary.

The new mouse action appears in the **Mouse Action** table.

Delete a Mouse Action

1 Open a session in Reflection.

2 Open the Mouse Mapper Dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Tools** tab, click **Mouse Mapper**.
Reflection Browser	On the **Reflection** menu, choose **Tools**, and then **Mouse Mapper**.
TouchUx	Tap the Gear icon and then select **Document Settings**. Under **Input Devices**, click **Manage Mouse Map**. Then choose whether to modify the current mouse map or create a new map.

3 From the **Mouse Mapper** dialog box, select the key combination you want to remove.

4 Click **Delete**, and then click **OK**.

5 Save your changes, as needed.

Restore the Default Mouse Map

If you have problems using a customized mouse map in a session document, you can restore the default mouse map.

To restore a default mouse map

1 Open the Document Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ⬚.
TouchUx	Tap the Gear icon and then select ⬚ **Document Settings**.

2 Under **Input Devices**, click **Manage Mouse Map**.

3 Click **Select another mouse map file**.

4 Click **Built-in**, and select Mouse.xmm from the list.

5 Click **OK**.

Related Topics

- "Add a Mouse Action" on page 66
- "Select a Mouse Map File Dialog Box" on page 276
- Select the Keyboard Map for a Session
- "Specify Trusted Locations Dialog Box" on page 426

Set up Productivity Features

Productivity features accelerate data entry and host navigation, maximizing user productivity, while reducing errors. Features such as Auto Complete, Auto Expand, Spell Check, Scratch Pad, Recent Typing, and Screen History enable users to save thousands of keystrokes throughout the day, freeing up time to serve customers more efficiently, and for more productive, revenue-producing activities.

In this Topic

- Customize Microsoft Office Productivity Features
- Integrate Host Data with Office Tools
- Enter Data with Recent Typing
- Take Notes with Scratch Pad
- Enter Data with Auto Complete
- Enter Data with Auto Expand
- Find and Fix Spelling Errors

- Create a Custom Spell Check Dictionary
- Turn off Screen History, Office Tools, and Productivity Features for Specific Fields

---

NOTE: VT sessions support only Office Tools integration, Scratch Pad, and the manual capture function of Screen History. Other productivity features are not available with VT sessions.

Video

▶️ Using Productivity Features (2:28)

Customize Microsoft Office Productivity Features

To customize productivity features

Open the Document Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click 📄.
TouchUx	Tap the Gear icon and then select 📄 **Document Settings**.

Select	To
Productivity defaults	Configure whether Recent Typing, Auto Complete, Auto Expand, and Spell Check are enabled by default.
Screen History	Set the maximum screens to capture, whether to capture manually only, and whether to clear screen history when disconnected.
Office tools	Specify PowerPoint presentation and Word templates.
	NOTE: If you specify templates, you will need to deploy the template files.
Recent Typing	Set the number of words to remember and whether to clear the list when disconnected.
Auto Complete	Configure Suggestions and whether to overwrite or insert suggestions.
Auto Expand	Set definitions for abbreviations you want to expand.
Spell Checking	Specify a custom dictionary and other options.

Integrate Host Data with Office Tools

You can send entire host screens or selected data directly to Microsoft Office products installed on your computer.

To copy and paste host screens or data, see "Copy and Paste Host Data" on page 34.

To send data from the current screen to an Office component

1 Navigate to the host data you want to send.

2 Select specific data to send.

   -or-

   To send the entire screen, don't select anything.

3 Do one of the following:

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	Click the **Office Tools** split button to open the Office Tools docking pane.
Reflection Browser	On the Reflection menu, choose **Send to**.
TouchUx	On the toolbar, tap the Office Tools icon.

4 Choose the Office component to receive the host data.

Choose	To do this
Email Message	Create an Outlook e-mail message that includes the selected host data.
Contact	Create a new contact in Outlook that includes the selected host data in the Notes field.
Appointment	Create an Outlook appointment that includes the selected host data in the message field.
Note	Create an Outlook "sticky" note that includes the selected host data.
Task	Create an unscheduled Outlook task that includes the selected host data in the task body field.
Word Processing Document	Create a Word document that includes the selected host data.

To send host screens from screen history to an Office component

1 Open the Screen History task pane.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Session** ribbon, click the Screen History button.
Reflection Browser	On the Reflection menu, choose **View** and then **Screen History**.
TouchUx	Tap the Wrench icon and then under **View**, choose **Screen History**.

2 From the toolbar in the **Screen History** task pane, click the **Office Tools** button.

3 Select the screens that you want to send.

4 From the **Document Type** list box, select the type of Office document that you want to create:

Choose	To do this
Word processing document	Create a Word document that includes the selected screens as text or images — specify which in the **Insert screens** list box.
Presentation	Create a PowerPoint presentation that includes the selected screens as bitmap images.
Email message	Create an Outlook e-mail message that includes the selected screens as text.
Note	Create an Outlook "sticky" note that includes the selected screens as text.

5 Click **OK**.

Related Topics

- "Copy and Paste Host Data" on page 34
- "Configure Office Tools Dialog Box" on page 280
- "Office Tools Dialog Box" on page 282
- "Capture Screen History" on page 38
- "Capture Screens Manually" on page 39

Enter Data with Recent Typing

Using the Recent Typing gallery or task pane, you can quickly view and select from a list of recently typed items, and send the selected string to the active document. This eliminates the need to manually re-enter information, saving time, and reducing errors when entering commonly-typed commands or field data.

NOTE

- This feature is not available with VT sessions.
- Typing is not captured in hidden-text fields such as passwords.

To enter data with Recent Typing

1 Navigate to the host field where you want to input the data.

2 Open the **Recent Typing** gallery or task pane.

3 Double-click the string you want to input.

The following commands are also available from the toolbar in the Recent Typing task pane:

Click	To do this
	Open a previously saved Recent Typing file.
	Save the contents of the Recent Typing task pane as a file (.RRTL). When you close your session, your recent typing items are not maintained unless you save them to a separate file.
	Delete the selected item.
	Clear all of the contents at once.
	Put the task pane into auto-hide mode. This collapses the task pane against the side of the application frame. (To re-open the task pane, mouse over the side of the frame.)

NOTE: You can use the keyboard to locate (and select) recently typed items in the list. For example, press the A key to locate the most recently typed item beginning with the letter A.

Related Topics

- "Configure Recent Typing Dialog Box" on page 282
- "Configure Productivity Defaults Dialog Box" on page 288

Take Notes with Scratch Pad

Use the Scratch Pad to keep notes associated with a session. From the task pane you can print or save the Scratch Pad notes as .RTF or .TXT files.

To reopen the file later, it must be saved in a trusted location.

To take notes with Scratch Pad

1 Open the Scratch Pad.

Open the Reflection **Scratch Pad** as follows:

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Session** ribbon, from the **Productivity** group, click the **Scratch Pad** button.
Reflection Browser	On the **Reflection** menu, choose **View**, and then **Scratch Pad**.
TouchUx	On the toolbar, tap the Wrench icon and then choose **Scratch Pad**.

2 Type your notes into the **Scratch Pad**.

3 Save your notes by clicking the **Save As** toolbar button.

The following commands are also available from the toolbar in the Scratch Pad task pane (You can also use common keyboard shortcuts like CTRL+A, CTRL+C, and so on):

Click	To do this
	Save the contents of the Scratch Pad task pane as a Rich Text File (.RTF) or as plain text (.TXT). When you close your session, your Scratch Pad is not maintained unless you save it to a separate file.
	Open any .RTF or .TXT file. The file must be in a trusted location.
	Print the contents of the Scratch Pad.
	Cut the selected item and copy it to the Clipboard.
	Copy the selected item to the Clipboard.
	Paste the contents of the Clipboard at the cursor location on the Scratch Pad.
	Clear all of the contents at once.
	Put the task pane into auto-hide mode. This collapses the task pane against the side of the application frame. (To re-open the task pane, mouse over the side of the frame.)

Related Topics

◆ "Specify Trusted Locations Dialog Box" on page 426

Enter Data with Auto Complete

The Auto Complete feature recalls what you type, and automatically makes suggestions to help populate fields as it learns common commands that are repeated. By default, typing is saved with the screen location, and suggested when you type at that screen location again.

NOTE: Auto Complete does not record typing in hidden-text fields such as passwords, nor does it offer suggestions to complete typing in such fields.

To enter data with Auto Complete, you must first have some suggestion data saved with your session. To generate suggestion data, type a string into a host field, followed by a Spacebaror a host key (Tab,field exit, AID key, and so on). The data is associated only with the field in which it was entered, unless you are configured to use field independent Auto Complete (select the **Make Suggestions from All Screen Data** option on the **Configure Auto Complete** dialog box).

This feature is not available with VT sessions.

To enter data with Auto Complete

1 Begin typing text into a host field.

   A pop-up window may appear with one or more suggestions, depending on your Auto Complete configuration and previous data entry activity.

2 If the suggestion is correct, press the ENTERkey to input the data.

-or-

If there are multiple suggestions, use the Up and Down Arrow keys on your keyboard to scroll through the suggestion list.

3 (Optional) To prevent the active suggestion from being suggested again in the current field, press the ESC key.

As you continue typing, the pop-up window will remain open until the word being typed no longer matches any previous suggestion data.

Related Topics

- "Configure Auto Complete Dialog Box" on page 283
- "Configure Productivity Defaults Dialog Box" on page 288

Enter Data with Auto Expand

Use the Auto Expand feature to add acronyms or shortcuts for long words, phrases, or complex repeat commands. The shortcut, when typed and followed by the Spacebar, automatically expands to the full word or phrase.

NOTE

- This feature is not available with VT sessions.
- Expansion does not occur in hidden-text fields such as passwords.

To enter data with Auto Expand

1 Build a dictionary in the Auto Expand Settings.

1a Open the Document Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click [icon].
TouchUx	Tap the Gear icon and then select [icon] **Document Settings**.

1b On the Settings dialog box, under **Productivity**, click **Configure Auto Expand**

1c From the Configure Auto Expand dialog box, create the desired Auto Expand definitions.

1d Click OK.

2 To insert data using Auto Expand, in the host field where you want the expanded data, type the abbreviation for an entry, and then press the Spacebar key.

The abbreviation is replaced with the Auto Expand definition you specified.

Related Topics

- "Configure Auto Expand Dialog Box" on page 285
- "Configure Productivity Defaults Dialog Box" on page 288

Find and Fix Spelling Errors

By default, spell check works as you type, using wavy underlines to indicate possible errors. If you prefer to wait until after you've finished entering content to make corrections, or you find the wavy underlines distracting, you can hide them.

NOTE: This feature is not available with VT sessions.

To show or hide spelling corrections as you type

1 Open the Configure Spell Checking dialog box.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Tools** ribbon, from the **Tools** group, click ᴬᴮꟲ **Spell Check**.
Reflection Browser	In the search box, enter S and then, under **Actions**, choose ᴬᴮꟲ **Spell Check Settings**.
TouchUx	Tap the Gear icon and select Document Settings. Then, under **Productivity**, select **Configure Spell Checking**.

2 From the **Configure Spell Checking** page, select or clear **Check spelling as you type**.

To correct spelling as you type

1 Open the Configure Spell Checking dialog box.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Tools** ribbon, from the **Tools** group, click ᴬᴮꟲ **Spell Check**.
Reflection Browser	In the search box, enter S and then, under **Actions**, choose ᴬᴮꟲ **Spell Check Settings**.
TouchUx	Tap the Gear icon and select Document Settings. Then, under **Productivity**, select **Configure Spell Checking**.

2 From the **Configure Spell Checking** page, select **Automatically correct spelling as you type**.

   Commonly misspelled words are corrected without prompt or indication as you type.

> **NOTE:** This feature is available only for English.

To correct an error

1 Right-click a word with a wavy underline, and then select the alternate spelling or correction you want.

2 If the spelling you want is not in the suggestion list, or if no suggestions appear, enter the correct spelling manually.

You can also add the item to a custom spell-check dictionary to make it available in the future. For more information, see "Create a Custom Spell Check Dictionary" on page 76.

> **NOTE:** If no suggestions appear, there aren't any available, or the suggestions available are too long to fit in the remaining space in the field.

Use the procedure below to check spelling on the entire screen, not just typed text.

To check and correct spelling on the whole screen

1 Select Check Screen.

The steps depend on your user interface mode:

User Interface Mode	Steps
Ribbon	On the **Session** ribbon, from the **Productivity** group, click ⬚ **Check Screen**.
Reflection Browser	In the search box, enter `C` and then, under **Actions**, choose ⬚ **Check Screen**.

Possible spelling errors are indicated with wavy underlines.

> **NOTE: Check Screen** is disabled if you have cleared the **Check spelling as you type** check box.

2 Right-click a word with a wavy underline, and then select the alternate spelling or correction you want.

Related Topics

 ◆ "Configure Spell Checking Dialog Box" on page 287
 ◆ "Create a Custom Spell Check Dictionary" on page 76
 ◆ "Configure Productivity Defaults Dialog Box" on page 288

Create a Custom Spell Check Dictionary

To increase the usefulness of the spell check feature, it helps to create a custom spell check dictionary, and add words to it that may be specific to your business or industry that are not included in the main dictionary. When you use spell check, both the main dictionary and your custom dictionary will be used.

NOTE

- ◆ This feature is not available with VT sessions.
- ◆ Spell check is not supported for Japanese.
- ◆ The spell check dictionaries are not used to correct spelling as you type. Instead, that feature uses a separate file of commonly misspelled words.

To create a custom spell check dictionary

1 Open the Configure Spell Checking dialog box.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Tools** ribbon, from the **Tools** group, click ᴬᴮꟼ **Spell Check**.
Reflection Browser	In the search box, enter Sand then, under **Actions**, choose ᴬᴮꟼ **Spell Check Settings**.
TouchUx	Tap the Gear icon and select Document Settings. Then, under **Productivity**, select **Configure Spell Checking**.

2 In the **Custom Dictionary File** field, type the path and filename that you want for your custom dictionary file.

   The filename must have an extension (we recommend `.tlx`).

3 Click **OK**.

   The file is created for you.

To add items to your custom spell check dictionary

1 On a host screen, right-click an item marked as misspelled that you want to add to your dictionary.

2 From the list that appears, choose **Add to Dictionary**.

Related Topics

- ◆ "Configure Spell Checking Dialog Box" on page 287
- ◆ "Find and Fix Spelling Errors" on page 75

Turn off Screen History, Office Tools, and Productivity Features for Specific Fields

You can turn off Screen History, Office Tools, and productivity features for fields that contain sensitive information (like user accounts) by setting Field Security for these fields.

When Field Security is on for a field, Screen History, Office Tools, and all of the productivity features are disabled for that field. These features still work for other fields where Field Security is off. Field Security settings are saved when you save your session files.

To Turn Field Security On

 ◆ In the program field you want to set, right-click and choose Field Security.

To Turn Field Security Off

 ◆ In a program field that has Field Security set to On, right-click and choose Field Security.

Change the Look and Feel of a Session

Change the look and feel of sessions, including color settings, cursor styles, sounds, underlining of input fields, and which dialog opens when Reflection starts. Control these options and more by creating and using custom theme files.

In this Topic

 ◆ Configure Color Settings

 ◆ Select a Cursor Style

 ◆ Map a Sound to an Event

 ◆ Underline Fields That Accept Input

 ◆ Create a New Theme File

 ◆ Specify which Dialog Box to Open when Reflection Starts

Video

▶️ Changing a Session's Look and Feel (1:10)

Configure Color Settings

You can change the colors for the application frame and Ribbon or for the session.

To change the color of the application frame and Ribbon

1 Open the Reflection Workspace Settings dialog box.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the File menu or the Reflection button 🌐 (if using the Office 2007 Look and Feel), choose **Reflection Workspace Settings**.
Reflection Browser	On the Reflection menu, choose **Settings** and then **Reflection Workspace Settings**.
TouchUx	Tap the Gear icon and then select **Reflection Workspace Settings**.

2 Under Workspace Settings, click **Configure User Interface**.

3 From the **Look and Feel / Color scheme** box, select the color scheme.

To change the colors used in a terminal session

1 Open the Document Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ⬚.
TouchUx	Tap the Gear icon and then select ⬚ **Document Settings**.

2 Under **Terminal Appearance**, click **Manage Themes**.

3 Click **Select another theme file**.

4 Select a theme with the colors and sounds you prefer.

5 Click **OK**.

Select a Cursor Style

You can set the cursor style and save it as a modification to your theme.

To select a cursor style

1 Open the Document Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ⬚.
TouchUx	Tap the Gear icon and then select ⬚ **Document Settings**.

2 In the Settings dialog box, click **Manage Themes**.

3 Select **Modify the currently selected theme file**.

4 In the Modify Theme dialog box, under **Cursor Style**, change the cursor settings and click **OK**.

Map a Sound to an Event

You can configure Reflection to play a sound when a session-level event occurs. This mapping is saved as a modification to your theme.

To map a sound to an event

1 Open the Document Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ⬚.
TouchUx	Tap the Gear icon and then select ⬚ **Document Settings**.

2 In the Settings dialog box, click **Manage Themes**.

3 Click **Modify the currently selected theme file**.

4 From the **Modify Theme** dialog box, under **Sounds**, select an item in the **Events** list.

5 Select a sound file to map to the selected event. (You can type the path and filename or click **Browse** to locate the file.)

Underline Fields That Accept Input

For IBM 3270 and 5250 terminals, you can set Reflection to underline fields that accept input. You can choose to always underline these fields, to allow the host to control whether they should be underlined, or to never underline them.

To specify whether to underline fields that accept input

1 Open a 3270 or 5250 terminal session.

2 Open the Document Settings dialog box.

The steps depend on your .

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ⬚.
TouchUx	Tap the Gear icon and then select ⬚ **Document Settings**.

3 Under **Terminal Configuration**, click **Configure Terminal Attributes(3270)** or **Configure Terminal Settings(5250).**

4 In the **Input field underlining** list, select whether to underline input fields.

Create a New Theme File

To create a theme file

1 Open the Document Settings dialog box.

The steps depend on your .

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ⬚.
TouchUx	Tap the Gear icon and then select ⬚ **Document Settings**.

2 Under **Terminal Appearance**, click **Manage Themes**.

3 Click **Create a new theme from an existing theme file** and then select the theme file to use as a template for creating a new theme file.

Built-In	Select this option to show the theme files distributed with Reflection.
Custom	Select this option to show the theme files that you've previously modified and saved. If the file you want doesn't appear in the list, click **Browse** to select it.
	NOTE: The file must be in a trusted location.
Use the new file in the current session document	Use the file you are about to create with the current session.

4 In the Modify Theme dialog box, select the settings for the theme file and then save the file.

Specify which Dialog Box to Open when Reflection Starts

By default, the **Create New Document** dialog box is displayed when you open the Reflection workspace.

To specify which dialog box to display when Reflection opens

1 Open Workspace Settings.

The steps depend on your .

User Interface Mode	Steps
Ribbon	On the File menu or the Reflection button ⊕ (if using the Office 2007 Look and Feel), choose **Reflection Workspace Settings**.
Reflection Browser	On the Reflection menu, choose **Settings** and then **Reflection Workspace Settings**.
TouchUx	Tap the Gear icon and then select **Reflection Workspace Settings**.

2 Under **Workspace Settings**, click **Configure Workspace Defaults**.

3 In the **When starting workspace** box, select one of the following options.

Select this	To do this
Show New dialog	Display the New dialog box used to choose which type of session to configure.
Show Open dialog	Display the Open dialog box used to choose a session document file.
Show nothing	Open the workspace without displaying a dialog box.
Run Startup Action	Specify an action or sequence of actions to perform when the workspace opens.

Related Topics

Select Alternate Icons

You can specify for Reflection to display simple, "flat" toolbar icons that support a modern look and feel or to display the legacy toolbar icons used on older versions.

The Reflection Ribbon, Browser, and TouchUx user interfaces display the modern, "flat" icons by default. Conversely, the Classic and Classic MDI interfaces display the legacy icons used on older versions by default.

You can switch these default settings as shown below.

To specify whether to use modern or legacy icons

1 Open Workspace Settings.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the File menu or the Reflection button 🌐 (if using the Office 2007 Look and Feel), choose **Reflection Workspace Settings**.
Reflection Browser	On the Reflection menu, choose **Settings** and then **Reflection Workspace Settings**.
TouchUx	Tap the Gear icon and then select **Reflection Workspace Settings**.

2 Under **Workspace Settings**, click **Configure User Interface**.

3 In the Configure User Interface dialog box, Under **UI Preferences**, select **Use alternate icons**.

The **Use alternate icons** option switches the default toolbar icon settings. With this option selected, the Ribbon, Browser, and TouchUx user interfaces use the legacy Reflection icons and the Classic and Classic MDI interfaces use the modern "flat" Reflection icons.

4 Restart the workspace.

Related Topics

- "Modify Theme Dialog Box (3270 Terminal Sessions)" on page 231
- "Modify Theme Dialog Box (5250 Terminal Sessions)" on page 233
- "Modify Theme Dialog Box (VT Terminal Sessions)" on page 235
- "Manage Themes Dialog Box" on page 229
- "Create a New Theme File" on page 80

Set up Custom Controls for your Program Screens

You can customize host sessions with Micro Focus Plus controls to provide a modern interface with new features and capabilities. You can also enhance your program interface using Reflection Hotspots (virtual buttons that appear over text in terminal sessions).

In this Topic

- Use Micro Focus Plus Screen Designer
- Enable and Define Hotspots
- Set up QuickPads
- Create a Custom Context Menu

Video

▶️ How to Use QuickPads in Reflection Desktop (4:18)

Use Micro Focus Plus Screen Designer

You can use Micro Focus Plus Screen Designer to customize host sessions and provide a modern interface with new features and capabilities. The Screen Designer provides a number of modern controls that you can add to your host screens to provide a more modern user experience for your host programs. Some examples of how you can use the Screen Designer include:

- Adding tool tips to fields to help your users get over the difficult spots in your application.
- Replacing old-style numbered option lists with more modern drop-down selection lists.
- Adding buttons to the host application's interface and programming them to start macros or perform other actions.
- Replacing manual entry of dates with a graphical calendar date-picker.

What you need to do to use the Screen Designer with Reflection

You'll need to follow this process to set up Screen Designer controls on a session.

NOTE

- ◆ Micro Focus Reflection Desktop Plus does not support Japanese and other languages that use double byte information.
- ◆ You can only customize screens for 3270 mainframe and 5250 IBM System i sessions.
- ◆ When you run a macro in Plus mode, controls do not appear on any customized screens until the macro reaches the final screen.

Get and save a screen history

1 Open a session and then select **Screen History**.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Session** ribbon, click the ⬚ **Screen History** button.
Reflection Browser	On the **Reflection** menu, choose **View** and then **Screen History.**
TouchUx	Tap the Wrench icon and then under **View**, select ⬚ **Screen History**.

2 Navigate through the screens you want to modernize.

3 On the Appearance tab, in the **Plus** group, from the **Plus** drop down list, select **Export History for Screen Designer**.

Use the Screen Designer to set up the controls on the screen

Follow this basic process to set up the controls. For detailed instructions, see the online Help provided with the Screen Designer.

1 On the Appearance tab, from the **Plus** drop down menu, select **Screen Designer**.

2 Create a new project, and then import the screen history.

3 Add static controls in the **Screen Design** view.

4 For dynamic control or conditional controls, create rules in the Rule Manager window.

5 Generate a Screen Designer customization file. Be sure to save the file in a trusted location, such as your user data directory (by default, this is `Documents\Micro Focus\Reflection\`).

The customization (`.rdar`) file is an archive file which contains the rules file (`.rsdo`) and resource files such as images, macros, and scripts.

Set up your session to use the controls

1 Open your session and select the Appearance tab.

2 On the **Plus** drop down list, choose **Select Plus Customization File** and then select the customization file you created for this session.

The controls you created are displayed on the session file screens.

Enable and Define Hotspots

Hotspots are virtual buttons that appear over text in terminal sessions. By using hotspots, you can control your terminal session with the mouse instead of the keyboard. Typically, clicking a hotspot transmits a terminal key or command to the host, but you can also configure hotspots to open a Web page, launch a macro, or perform a variety of other actions.

You can create new hotspots files or set sessions to use customized hotspot files that you have used in other sessions.

To create and configure a customized hotspots file

1   Open the Document Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ⬚.
TouchUx	Tap the Gear icon and then select ⬚ **Document Settings**.

2   Under **Terminal Appearance**, click **Manage Hotspots**.

3   Click **Create a new hotspots file from an existing hotspots file**.

4   In the **Create a New Hotspots File** dialog box, select the type of hotspots file (built-in, Custom, or the new file for the current session) to use as a template for creating a new hotspots file.

5   In the Modify Hotspots dialog box, under **Hotspot text**, enter the text for the hotspot.

6   Under **Select an action to map to the hotspot**, select an action to map to and configure the action.

7   When prompted, save the new hotspot file.

8   On the **Quick Access Toolbar**, click the **Save** ⬚ button to save the session.

The session is automatically configured to point to the new hotspot file.

To set up a session to use a customized hotspots file

1   Make sure the hotspots file is in a trusted location.

2   Open the Document Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ⬚.
TouchUx	Tap the Gear icon and then select ⬚ **Document Settings**.

3   Under **Terminal Appearance**, click **Manage Hotspots**.

4   Click **Select another hotspots file**.

5 Select **Custom** and browse to the file you want to use.

The selected file is displayed under **currently selected file**.

6 Save the session.

The session is configured to point to the new hotspot file.

To enable hotspots and specify which mouse actions trigger them

1 Open the **Document Settings** dialog box.

2 Under **Terminal Appearance**, click **Set Up Hotspot Display Settings**.

3 Select **Enable all defined hotspots**.

4 Under **Mouse Activation**, configure the mouse actions that you want to trigger your hotspots.

Set up QuickPads

A QuickPad is a small window that you can load during a session. QuickPads can contain text, buttons, bitmaps, icons, and other graphic elements. The buttons and icons on QuickPads can be linked to any of the Actions available in the Select Action Dialog Box (page 253).

▶ How To Use QuickPads in Reflection Desktop (4:07)

To create a QuickPad

1 Open the **Document Settings** dialog box.

The steps depend on your user interface mode (page 216).

Ribbon	With a session open, from the **Quick Access Toolbar**, click [icon].
TouchUX	With a session open, tap the Gear icon [icon] and then select [icon] **Document Settings**.
Classic	With a session open, do one of the following: ◆ If you are using a VT session, select **View Settings** on the **Setup** menu. ◆ If you are using another type of session, go to **Options** from the **Settings** menu.

2 Under **Terminal Appearance**, click **Manage QuickPads**.

3 Click **Create a new QuickPad**.

4 Use the QuickPad Designer to configure your QuickPad.

5 Click **OK**. Use the Save As dialog box to save your QuickPad file (`*.rqpx`).

To add a QuickPad to your session

1 From the **Manage QuickPads** dialog box, click **QuickPad Selection**.

2 In the **Available QuickPads** list, select the QuickPad and click **OK**.

The QuickPad is now set to display when you open new sessions using this document.

Create a Custom Context Menu

You can create custom context menus for legacy hot lists or for other types of frequently used commands. After you create a custom context menu, you can map a mouse action to open the new menu.

1 Open the Context Menu Editor.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	Click the Appearance tab and in the **Menus** group, select **Context Menu**.
Reflection Browser	On the Reflection menu, choose **View** and then choose **Context Menu**.
TouchUx	Tap the Wrench icon and then under **View**, select **Context Menu**.
Classic IBM	On the **View** menu, choose **Context Menu**.
Classic VT	On the **Setup** menu, choose **Context Menu**.

2 At the top of the **Context Menu** dialog box, click **Add** and enter the name of your context menu.

3 Add the menu items and separators for your new menu.

4 Under **Menu Item** settings, enter the label and select an action for each item.

5 Click **OK** to save the new menu.

Next, you'll want to make a right-click open the new custom context menu instead of the default.

1 Open the Mouse Mapper dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Tools** tab, click **Mouse Mapper**.
Reflection Browser	On the **Reflection** menu, choose **Tools**, and then **Mouse Mapper**.
TouchUx	Tap the Gear icon and then select **Document Settings**. Under **Input Devices**, click **Manage Mouse Map**. Then choose whether to modify the current mouse map or create a new map.

2 Under **Mouse Mapper**, for **Key Combination**, select **Right** and then click **Modify**.

3 From the list of actions, select **Show Specific Context Menu**.

4 On the right, from the **Context Menu**, choose the name of the new custom context menu.

Record, Run, and Edit VBA Macros

You can create and run Visual Basic for Applications (VBA) macros to simplify and automate routine tasks.

- ◆ "Running VBA Macros" on page 88
- ◆ "Recording and Deleting VBA Macros" on page 91
- ◆ "Creating a Macro in the Visual Basic Editor" on page 93
- ◆ "Editing a Macro" on page 94
- ◆ "Run a Startup Macro" on page 94
- ◆ "Set up Macros that Run Before or After a Host Connection" on page 95
- ◆ "Naming Macros" on page 96

Video

▶️ Use the Macro Panel(1:52)

▶️ How to Record a Macro When Using the Reflection Desktop Ribbon(1:14)

▶️ How to Record a Macro When Using the Reflection Desktop Classic Interface(2:31)

▶️ Running Extra! Macros in Reflection Desktop (3:06)

Running VBA Macros

You can run VBA macros saved in your session document file from the Macro Panel. This is a convenient way to keep track of and run your macros without adding buttons to the ribbon. You can also run other types of macros from this panel after you run them from the Run Macro dialog box.

Running macros with the Macro Panel

You can use the Macro Panel to run VBA macros saved in your session document file or to run other macros, such as referenced macros, EML macros, or macros created with other products, that you have previously run on that session. The Macro Panel is a convenient way to keep track of and run macros that apply to a session without adding buttons to the ribbon. It displays only the macros that apply to the session that has focus.

To run macros from the Macro Panel

1 On the Session tab, in the Macros group, click Show Macro Panel.
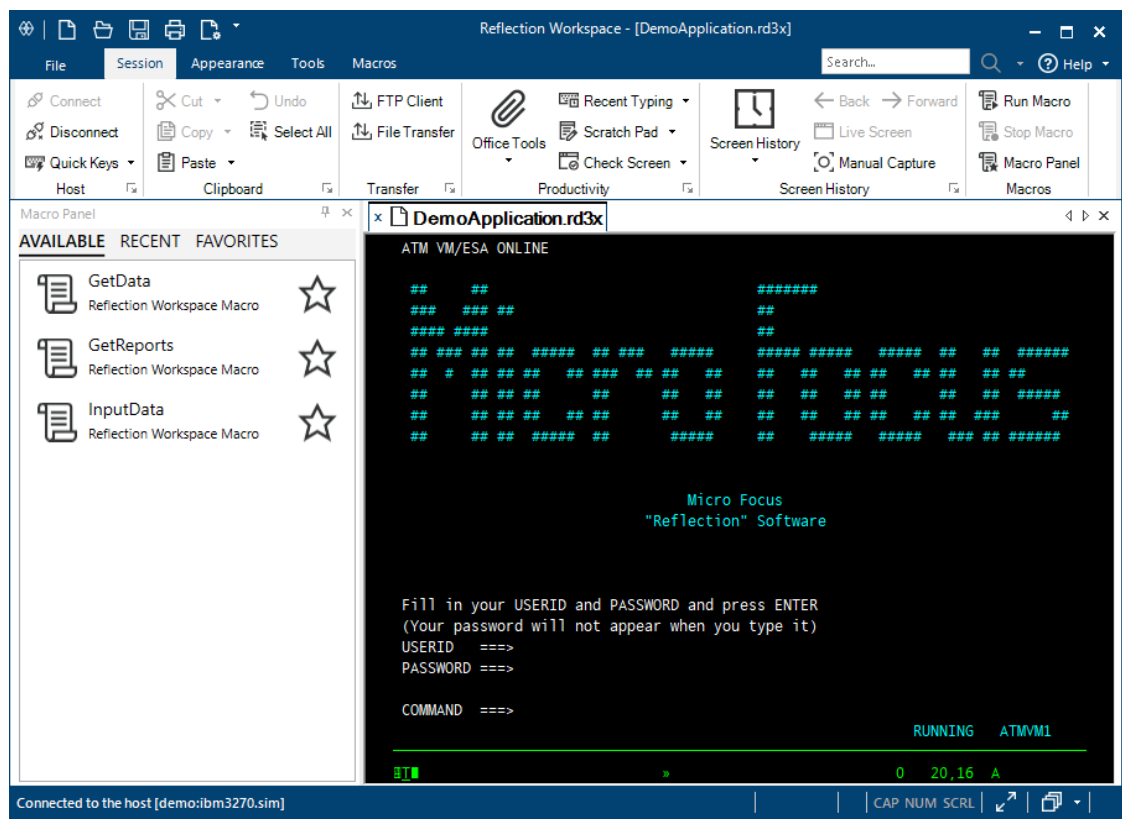
The Macro Panel has three tabs:

The Available tab shows the VBA macros that are saved in the session document file.

NOTE: The Available tab does not show EML macros, macros created with other products, or other macros that are not saved in the session document file.

The Recent tab shows all macros that you have previously run in this session. This includes VBA macros as well as other supported macros that you have run, such as EML macros or macros created with other products.

The Favorites tab shows the all the macros that you have marked as favorites.

2 To run a macro, mouse over the macro you want to run and then the Play ▶ button on the left side of the macro.

3 To stop a macro, click the Stop ⊗ button next to the macro.

4 To get more information about a macro, mouse over the macro.

For VBA macros, a tooltip shows the VBA project and module that the macro is in.

For other macros, a tooltip shows the type of macro and its fully qualified file name.

Video

▶ Use the Macro Panel(1:52)

Running macros from the Run Macro dialog box

You'll need to use the Run Macro dialog box to run macros that are not saved in the session document file the first time you run these macros. After you run a macro once, you can run it from the Macro Panel's Recent tab.

To run a macro from the Run Macro Dialog Box

1 Open the Run Macro dialog box.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Session** tab, from the **Macros** group, click **Run Macro**.
Classic and Classic MDI	On the **Macro** menu, choose **Macros**.

2 Select the type of macro you want to run and select to open it.

   The macro runs.

   NOTE: After you run the macro once, you can run it from the Macro Panel's Recent tab.

Running macros created in other products

You can run VBA macros created in Reflection, and most macros created with Extra! and legacy Reflection products. You can also run the majority of macros created with the Micro Focus Rumba, IBM Personal Communications, OpenText HostExplorer, and Brandon Systems\Jolly Giant QWS3270 products. However, you can only run macros in trusted locations.

Several macro-related actions (such as, Run a Reflection Workspace Macro) are available from the **Select Action** dialog box.

You can also run a macro by mapping an action to a control. For more information, see "Add a Button to Run a Macro" on page 102.

To run macros created with other products

1 Open the Run Macro dialog box.

   1a The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Reflection Ribbon	On the **Macros** tab, from the **Advanced** group, click **Run Macro**.
Reflection Browser	On the **Reflection** menu, choose **Tools**, **Macro** and then **Run Macro**.
TouchUx	Tap the Wrench icon and then under **Macro**, select **Show Run Macro Dialog**.

2 From the **Run Macro** dialog box, select the macro you want to run.

NOTE: Legacy macro options are available only if compatibility features are installed. In addition, to run Extra! and legacy Reflection macros from external files, you must specify, from the **Set Up API and Macro Security** dialog box, the type of legacy macro you want to run.

Reflection Workspace Macro	Shows macros in the active session document. Select to run macros created in Reflection or 2007 (SP1) documents.
	To run a macro in the Common project and other documents, select the **<All Standard>** option from the **Macros in** menu:
Legacy Reflection Macro in This File	Select to run legacy macros in the active document. These macros include legacy settings files (.rsf, .r2w, or .r4w), and in Reflection, session documents (.rd3x, .rd5x, .rdox) that were previously converted from settings files.
Legacy Reflection Macro in Another File	Select to specify and run a macro in a SharedMacro file (.rma) or a settings file (.rsf, .r2w, or .r4w).
Legacy RB Macro	Select to specify and run a Reflection Basic macro (.rbs).
Legacy RCL Script	Select to specify and run a legacy RCL script. Available only for use in VT session documents.
Extra! Macro	Select to specify and run an Extra! macro file (.ebm).
Rumba Macro	Select to specify and run a Micro Focus Rumba macro file (.rmc).
QWS Macro	Select to specify and run a Brandon Systems\Jolly Giant QWS3270 macro file (.jgs).
IBM Personal Communications Macro	Select to specify and run an IBM Personal Communications macro file (.mac).

3 If you can't find a **Workspace** macro, select **Set Up VBA References** in the Settings window to open the Add VBA Reference macro dialog box and then check the list for missing references (indicated by the 🚫 button). After you correct the problem (usually a missing file or a disconnected network drive), close and reopen your session.

Recording and Deleting VBA Macros

You can record a VBA macro to automate your interaction with host applications, including:

- Sending data to, or typing text in, a host application.
- Cutting, copying, or pasting text or data from one host application to another.
- Switching tabs to move from one host application to another.
- Selecting text with a mouse or clicking the mouse to move the cursor (mouse clicks are recorded as cursor positions.)

You cannot record:

- Interaction with Reflection settings and Productivity features (such as Spell Check, Auto Expand, and Auto Complete).
- Connecting to or disconnecting from a host.

- Interaction with Web applications.
- Cutting or pasting from a host to an external application (for example, Notepad).

Best Practices for Recording Macros

Use the following best practices to carefully record your macro will help prevent problems that can occasionally occur when using a slower network connection. Typing very fast while recording or "typing ahead" in a session, while connected with a slow network connection can cause your macro to play back in unexpected ways. Following these best practices will lead to the best results.

- Plan in advance of the recording to make sure you know the steps you will follow, which keys you will press, and which host screens are anticipated.
- While recording the macro, after pressing a key to submit data to the host, wait for the next host screen to fully appear (sometimes even waiting a few extra seconds) before pressing the next keys.
- If your macro doesn't play back like you expect, delete the macro and carefully record it again using slow and deliberate steps.

Recording a macro slowly and carefully does not cause the macro to run with reduced performance, as macros always run at the fastest speed possible during playback. Recording a well thought out and planned macro will lead to the best results.

To record a macro

1 **Select Record Macro**.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Macros** tab, from the **Advanced** group, click **Record VBA**.
Reflection Browser	On the **Reflection** menu, choose **Tools**, **Macro** and then **Record VBA Macro**.
TouchUx	Tap the Wrench icon, and then under **Macro**, select **Record VBA Macro**.

2 Perform the task(s) that you want to automate.

3 (Optional) If you need to interrupt the recording to perform another task, click **Pause Recording**. When you are ready to resume recording, click **Pause Recording** again.

4 When you are finished recording the macro, click **Stop Recording**.

The **Recording Complete** dialog box appears.

5 Name the macro and choose the location where you want to save it.

6 If you want to run the macro every time the session connects, select **Make this the Connect Macro**.

NOTE: You can fine-tune recorded macros by using the Visual Basic Editor. For more information, see Edit a Macro. (page 94)

7 If your macro doesn't play back like you expect, delete the macro and follow best practices to carefully record the macro again.

To delete a macro

1 Open the Run Macro dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Session** tab, from the **Macros** group, click **Run Macro**.
Classic and Classic MDI	On the **Macro** menu, choose **Macros**.

2 Select Reflection Workspace Macro.

3 In the Macros dialog box, select the macro you want to remove and then click **Delete**.

Video

▶ How to Record a Macro When Using the Reflection Desktop Ribbon(1:14)

▶ How to Record a Macro When Using the Reflection Desktop Classic Interface(2:31)

Creating a Macro in the Visual Basic Editor

Whenever possible, create macros in Modules. Doing so will add to the integrity and stability of your program. The exception to this rule is event procedures, which are added directly to Reflection objects.

To create a macro in the Visual Basic Editor

1 In Reflection, open a session document.

2 Open the Visual Basic Editor.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Reflection Ribbon	From the **Macros** tab, click **Visual Basic**.
Reflection Browser	On the **Reflection** menu, choose **Tools**, **Macro** and then **Visual Basic**.
TouchUx	Tap the Wrench icon and then under **Macro**, select **Visual Basic**.

The session document appears as a project in the **Project Explorer**; for example, Project (`My Session.rd3x`).

3 In the **Project Explorer**, select the project in which you want save the macro, and then choose **Insert** > **Module** to create a new module.

4 Double-click the module you created.

The **Code** window opens.

5 Choose **Insert**> **Procedure**, type a name in the **Name** box, and then click **OK**.

The name you choose must follow the Visual Basic naming conventions for macros. For further information, see "Naming Macros" on page 96.

6 Type code for your macro between the `Sub` (or `Public Sub`) and `End Sub` statements.

Context-sensitive Help is available for Visual Basic commands. Position the insertion point within a command and press F1.

Editing a Macro

Use the Visual Basic Editor to edit Reflection macros.

To edit a macro

1 Open the Visual Basic Editor.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Reflection Ribbon	From the **Macros** tab, click **Visual Basic**.
Reflection Browser	On the **Reflection** menu, choose **Tools**, **Macro** and then **Visual Basic**.
TouchUx	Tap the Wrench icon and then under **Macro**, select **Visual Basic**.

The **Macros** dialog box appears.

2 In the **Macro name** box, select the name of the macro to edit and click **Edit**.

3 In the Visual Basic Editor, type in or edit the macro commands.

4 From the **File** menu, choose **Save**.

Run a Startup Macro

You can set up a Visual Basic for Applications (VBA) macro to run when a Reflection workspace starts, rather than when a session opens and connects to the host.

This allows you to gather information about how users will connect and then use that information to configure session settings.

For example, you can create a startup macro to perform tasks such as:

- displaying a VBA UserForm to gather information from the user before connecting to the host
- reading from an `.ini` file
- checking for host or router availability

◆ configuring Reflection settings

> **CAUTION:** You can configure only macros in the Common project to run when the workspace starts. Do not configure the "Run Reflection Workspace Macro" action to run a macro present in a session document (`rd0x`, `rd3x`, `rd5x`). This prevents Reflection from starting properly.

To set up a startup macro

1 Open the Reflection Workspace Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the File menu or the Reflection button (if using the Office 2007 Look and Feel), choose **Reflection Workspace Settings**.
Reflection Browser	On the Reflection menu, choose **Settings** and then **Reflection Workspace Settings**.
TouchUx	Tap the Gear icon and then select **Reflection Workspace Settings**.

2 Under **Workspace Settings**, click **Configure Workspace Settings**.

3 Under **Workspace and Documents**, in the **When starting workspace** list, select **Run Startup action**.

4 Click **Select Action**.

5 Under **Action,** select **Run Reflection Workspace Macro**.

6 Under **Action parameters**, choose **Select macro**.

7 In the **Select a macro** box, select the macro you want to run when Reflection starts.

Set up Macros that Run Before or After a Host Connection

If you have created a macro for your session or workspace, you can set up the session to run a connection macro.

To set up a connection macro

1 Open the Document Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click .
TouchUx	Tap the Gear icon and then select **Document Settings**.

2 On the Settings… dialog box, do one of the following

◆ (VT)click **Configure Connection Settings**.

◆ (3270 or 5250), click **Configure Advanced Connection Settings**.

3 Under **Connection Action**, select whether to run the macro before or after the initial connection.

4 Click **Select Action** and select the macro to run.

Naming Macros

Observe the following rules when you name Visual Basic macros (including procedures, constants, variables, and arguments):

- Use a letter as the first character. (Names aren't case sensitive, but they preserve capitalization.)
- Use only alphanumeric characters and the underscore character (_). Spaces and other symbols are not allowed.
- Use fewer than 255 characters.
- Avoid names that match Visual Basic or Reflection commands. Or, if you do use a macro name that is the same as a command, fully qualify the command when you want to use it. (To do this, you need to precede the command name with the name of the associated type library. For example, if you had a macro named Beep, you could only invoke the Visual Basic `Beep` statement using VBA. `Beep`.)
- Give unique names to macros within a single module. Visual Basic doesn't allow you to have two macros with the same name in the *same* code module. However, you can have two macros with the same name if they are in *different* code modules. For example, although you could *not* have two macros named StartUp in the same code module, you could have two macros named StartUp if they were in different code modules. To call a macro with a duplicate name that is in another code module, you must fully qualify the macro name. (For example, Module1.StartUp invokes the StartUp macro in Module1.)

Set up Actions for Reflection Events

Using the Events Mapper, you can configure Reflection to initiate Reflection actions, such as Reflection macros, and menu and terminal commands when an event is encountered during a host session. This makes it possible to monitor Reflection/host interactions and synchronize Reflection commands with a defined group of host session events.

You can associate events with a Reflection command, Reflection macro, terminal keystroke, or any combination of these. There are 17 events you can select with which to associate actions. Each event can execute once per session, or every time the event occurs. Events can also be defined so that they execute one after another, in the order shown in the Events list in the Events Mapper dialog box.

To use the Events Mapper to assign actions to events, see "Using the Events Mapper" on page 97.

In this Topic

- "Cursor Events" on page 97
- "String Related Events" on page 98
- "Time Related Events" on page 98
- "Keyboard Events" on page 99
- "Changes in State Events" on page 99

Using the Events Mapper

You can use the Events Mapper on any of the alternate Reflection interfaces. Use the Events Mapper to assign actions to events, determine whether the events should be canceled or removed after the first time they are handled, and order the events.

To set up actions for events

1 Open the Events Mapper as follows:

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the Tools tab, click **Events Mapper**.
TouchUx	Tap the Wrench icon and then select **Events Mapper**.
Reflection Browser	On the Reflection menu, choose **Tools** and then **Events Mapper**.
Classic	On the View menu, select **Events Mapper**.

2 To add an event, click **New** and then follow the instructions in the Event Editor wizard to select the type of event, specify the parameters for the event (if required), add an action for the event, and determine whether to disable it after it runs the first time. When you are through, name the event you created.

The event is displayed in the Events Mapper Events list. Note that the checkbox next to the event is selected. This indicates that the action associated with the event will be performed the next time the event is handled. If you have selected to disable the "event state after the action is complete", this checkbox will be automatically unselected after the event runs.

3 To insert a copy of an event, select the event in the Events list and then click **Duplicate**.

4 Before you save the session document file, be sure to select the checkboxes next to the events in the Events list (if you want them to run the next time you open the session).

Cursor Events

Cursor related events occur when the cursor enters or leaves a field or screen position. You can set up these events to execute at a specific point (row and column) or for a specific row or a specific column.

This example shows the Events Mapper settings used to set up the **When the cursor enters a position** event so that a Web page opens when you click on the top row of the screen. In our example, we open microfocus.com but you could use this approach to open an internal Web page that included Help or other types of information related to the session.

Name	Description	Action
Open Web page	When the cursor enters the position row 1, any column	Open URL (http://www.microfocus.com/, NewTab, _none_)

String Related Events

String related events occur when text is received from the host or displayed on the screen.You can set up string events to perform actions when a string is entered or displayed on the screen or a string is received from the host.

You set up string related events to detect the string you enter at any position on the screen or only when the string is at a specific screen position.

NOTE: Reflection initiates the specified event even if the string is masked (invisible). String detection is case sensitive and does not include line wraps.

This example shows the Events Mapper settings used to navigate through two host screens.

The first event in the sequence (**When string received from host**) occurs after the user logs on. It is mapped to the SendText action and configured to send the "demo" command to the host to navigate to a screen of program demos.

The next event (**When screen text is recognized**) occurs on the subsequent screen. It is also mapped to the SendText action and configures it to send the option list command "3" to the host to navigate to another screen. Both events are set up to be triggered once and then disabled.

Name	Description	Action
First screen	When the text "syl_SYSTEM" is received from the host	Send Text (demo<CR>)
Second screen	When the text "2 and 4" appears on the screen at any row, any column	Send Text (3<CR>)

Time Related Events

Time related events include specific times of day, elapsed time (e.g., every half hour), or time outs from lack of activity. These events require definition of either when the event should occur, or after how much time the event should occur.

NOTE: The time of day is taken from the PC, and not the host. If the host is located in a different time zone than the PC, you must make an allowance for this.

The following example Events Mapper settings, uses the **When the absence of activity for a specified duration** event to disconnect the session after 30 minutes of inactivity.

Name	Description	Action
Disconnect if no activity	After 0 hours, 30 minutes, and 0 seconds without receiving any characters from the host	Disconnect

Keyboard Events

Keyboard related events occur when the keyboard is unlocked or when a key is pressed.

Changes in State Events

Changes in session state include connecting and disconnecting, screen changes, completion of a file transfer, and entering or exiting a terminal block mode.

This example shows the Events Mapper settings you would use to run a file transfer macro at the end of the day, disconnect from the host after the file transfer is complete, and then shut down the workspace. To do this, it uses the **At a specific time of day** event, set to execute a macro that transfers the file. Next, the **When a file transfer has finished** event is set to execute the Close action to close the session. Finally, the same type of event, **When a file transfer has finished**, is set to execute the Exit action that closes the workspace.

The Events list settings for this sequence are shown below:

Name	Description	Action
Run file transfer macro	When the time of day is 5:00:00 PM	Run Reflection Workspace Macro (Module1.TransferFile, local_proj, False,)
Close the session	When file transfer is done	Close
Exit the workspace	When file transfer is done	Exit

NOTE: You can use two or more of the same events in a sequence just we did in this example; this requires only that they be enabled, and ordered correctly in the Events list.

Customize the Ribbon

Customize the ribbon to add, remove, or modify ribbon controls, import legacy toolbars, change the Quick Access Toolbar, and minimize the ribbon.

In this Topic

- Customize the Quick Access Toolbar
- Add Controls to the Ribbon
- Remove Controls from the Ribbon
- Modify Existing Controls on the Ribbon
- Move Controls on the Ribbon
- Restore the Default Ribbon
- Import Legacy VT Toolbars to the Ribbon
- Minimize the Ribbon

Video

Using the Reflection Ribbon(2:48)

Customizing the Ribbon (3:04)

Using the Quick Access Toolbar (1:12)

Customize the Quick Access Toolbar

The Quick Access Toolbar contains a set of controls that you can use to perform common tasks and access document settings. It is located at the top of the Reflection window.

The Quick Access Toolbar

You can add button controls to the Quick Access Toolbar from the Ribbon interface or from the workspace menu. You can also add custom button controls that you have created.

NOTE: You can add only simple button controls to the Quick Access Toolbar. You cannot add complex buttons or other interface items.

To add or remove Quick Access Toolbar buttons

With a session open, add or remove Quick Access Toolbar button controls as follows:

To	Do this...
Add a button control from the workspace menu.	1. Open the Reflection Workspace menu. 2. On the menu, right click on the button control you want to add, and then select **Add to Quick Access Toolbar**.
Add a button control from the Ribbon	On the Reflection Ribbon, right click on the button control you want to add, and then select **Add to Quick Access Toolbar**.
Add a custom button control	1. Click the Quick Access Toolbar menu, and then select **Add an Action**. 2. In the Select Action Dialog box, under **Action**, select an action and then specify action parameters (if required).
Remove a button control	On the Quick Access Toolbar, right-click the button control you want to remove and then select **Remove from Quick Access Toolbar**.

The Quick Access Toolbar button controls that you add are automatically saved in your workspace file and are displayed the next time you open Reflection.

You can change the action that a button on the Quick Access Toolbar (QAT) is associated with. You can also move the button to change its position on the toolbar.

To edit a QAT button

1. On the QAT, right click on the button you want to edit and select **Modify**.

2. In the Select Action dialog box, select the action you want to associate with the button and click **OK**.

To move a QAT button

◆ On the QAT, drag the button to the position you want to move it to.

Add Controls to the Ribbon

With the **UI Designer**, you can add tabs, groups, buttons, and menus to the Ribbon. You can implement most tasks as a button control, a menu item, or as a combination of the two.

Button groups have the most flexibility of all controls because they can include both buttons and menus. If you need more space for controls, you may want to create a new tab, and add groups to it. A group is a structure to which you can add buttons, button groups, and menus.

To access the **UI Designer**, select the **Appearance** ribbon, and then, from the **Menus** group, click the **UI Designer** button.

To	Insert this type of control
Perform a single task or action	Button (page 102)
Run a macro	Button (page 102)
Add a group of three buttons	Button group (page 104)
Perform an action and open a menu	Split button (page 103)
Add a menu of options, thumbnails, or commands	Gallery (page 103)
Open a dialog box from a group	Dialog launcher (page 105)
Create a container to which you can add other controls, such as buttons, button groups, and split buttons	Group (page 104)
Create a new category on the Ribbon for custom controls	Tab (page 105)

NOTE: The UI Designer is just one way to create controls — the Context Menu Editor, Keyboard Mapper, Mouse Mapper, and Hotspots provide other ways for you to run favorite macros and actions.

Add a Button that Opens a Session Document

You can add a button to the Quick Access Toolbar (QAT) that opens a session document. (You can also map this action to a Ribbon button or a keyboard shortcut.)

To add a QAT button that opens a session document

1   From the Quick Access Toolbar, select to add an action.

2   In the Add an Action dialog box, select **Open Document**.

3   Browse to the session document file you want to open when the button is clicked.

Add a Button

Use the **Button** control to add a button that performs a single task or action.

To add a button

1 On the **Appearance** tab, click **UI Designer**.

2 From the **Design View** pane, from the Ribbon simulation, select the tab and group to which you want to add the control.

   To select a group, click the group name. Create a new group, if needed.

3 From the **Insert Controls** pane, click **Button**.

4 From the **Settings** pane, set the action and other properties for the new button that appears on the Ribbon.

5 Click **OK**.

Add a Button to Run a Macro

With the UI Designer, you can add a button or other control that runs a macro or a macro-related action to the Ribbon. All supported macros, including RCL scripts and legacy macro editors, are available as actions. Legacy compatibility features must be installed for these options to appear in the Actions list. For more information, see the Reflection Administrator's Reference.

NOTE: The UI Designer is just one way to create controls — the Context Menu Editor, Keyboard Mapper, Mouse Mapper, and Hotspots provide other ways for you to run favorite macros and actions.

To add a button that runs a macro-related action

1 On the **Appearance** tab, click **UI Designer**.

2 From the **Design View** pane, from the Ribbon simulation, select the tab and group to which you want to add the control.

   To select a group, click the group name. Create a new group, if needed.

3 From the **Insert Controls** pane, click **Button**.

4 From the **Settings** pane, click the **Select Action** button.

5 From the **Action category** menu, choose **Macro**.

6 Select an action from the **Action** list.

   If you selected an action that runs a macro, select the appropriate options:

To	Choose
Select a macro (or open a file that contains macros) each time you click the button	**Select macro when action occurs**
Specify a macro that runs automatically each time you click the button	**Select macro** You can enter command-line arguments for the macro in the **Macro data** field

7 From the **Settings** pane, set the properties for the new button that appears on the Ribbon.

8 Click **OK**.

9 If prompted, type a new filename for the custom ribbon and then save the file.

The button is saved to a custom ribbon file that you can use in other session documents.

Add a Button with an Action and a Menu

A split button includes a functional button and a menu. Split buttons look like galleries except that they perform an action in addition to opening a menu. For an example of a split button, see the **Screen History** control — when clicked, the button opens an option pane and the menu shows a history of recorded screens.

To add a split button

1 On the **Appearance** tab, click **UI Designer**.

2 From the **Design View** pane, from the Ribbon simulation, select the tab and group to which you want to add the control.

To select a group, click the group name. Create a new group, if needed.

3 From the **Insert Controls** pane, click **Split Button**.

4 From the **Subitems Collection Editor** dialog box, click **Add,** and then select **Button**.

5 Repeat the previous step to add as many buttons as you want to appear in the menu.

6 With a button selected in the list, set the action and other properties.

7 When you have finished adding and configuring buttons, click **OK**.

The **Subitems Collection Editor** dialog box closes.

8 From the **Settings** pane, set the action and other properties for the new split button that appears on the Ribbon.

9 Click **OK**.

Add a Menu that Holds Buttons

Use the **Gallery** control to add a menu of options to the Ribbon.

NOTE: To add a button that performs an action in addition to opening a menu, use the **Split Button** control.

To add a gallery

1 On the **Appearance** tab, click **UI Designer**.

2 From the **Design View** pane, from the Ribbon simulation, select the tab and group to which you want to add the control.

To select a group, click the group name. Create a new group, if needed.

3 From the **Insert Controls** pane, click **Gallery**.

4 From the **Subitems Collection Editor** dialog box, click **Add,** and then select **Button**.

5 Repeat the previous step to add as many buttons as you want to appear in the menu.

6 With a button selected in the list, set the action and other properties.

7 When you have finished adding and configuring buttons, click **OK**.

The **Subitems Collection Editor** dialog box closes.

8 Specify the appearance of the gallery by doing one of the following:

◆ Select **Change settings**, and then type the label, tooltip, and description you want.

-or-

◆ Click **Select Action**, and then select an action from which to use the label, tooltip, and description.

9 Click **OK**.

Add a Group

A group provides a container for controls on the Ribbon. For an example of a group, see **Host** or **Clipboard** on the **Session** ribbon.

To add a group

1 On the **Appearance** tab, click **UI Designer**.

2 From the **Design View** pane, from the Ribbon simulation, select the tab to which you want to add a new group of controls.

3 From the **Insert Controls** pane, click **Group**.

4 Enter a label for the group name.

5 Add controls to the group by clicking them in the **Insert Controls** pane.

6 Specify control settings, and then click **OK** to save your changes.

Add a Group of Buttons

You can stack up to three controls — buttons, split buttons, and galleries — in a button group. For an example of a button group on the Ribbon, see the **Host** group on the **Session** ribbon: **Connect**, **Disconnect**, and **Quick Keys** are combined in a single button group.

To add a button group

1 On the **Appearance** tab, click **UI Designer**.

2 From the **Design View** pane, from the Ribbon simulation, select the tab and group to which you want to add the control.

To select a group, click the group name. Create a new group, if needed.

3 From the **Insert Controls** pane, click **Button Group**.

4 From the **Subitems Collection Editor** dialog box, click **Add** and then select the item you want.

5 Repeat the previous step to add additional buttons, split buttons, or galleries (up to three items total).

6 With a button, split button, or gallery selected in the list, set the action and other properties.

When you have finished adding and configuring items to the group, click **OK** to close the **Subitems Collection Editor** dialog box.

7 Click **OK**.

Add a Dialog Launcher to a Group

Groups can include a dialog launcher control in the lower-right corner. This control typically opens settings or performs other tasks relevant to the group.

To add a dialog launcher

1 On the **Appearance** tab, click **UI Designer**.

2 Do one of the following:

  ◆ Create a new group by clicking **Group** in the **Insert Controls** pane.

    -or-

  ◆ Select an existing group from the **Design View** by clicking the group name.

3 With the group selected, from the **Settings** pane, select **Show dialog launcher button** to enable the settings.

4 From the **Settings** pane, to set the action and other properties for the new dialog launcher that appears on the Ribbon, click **Select Action**.

5 Click **OK**.

Add a Tab

Add a new tab to create a new category on the Ribbon for custom controls.

To add a tab

1 On the **Appearance** tab, click **UI Designer**.

2 In the **Insert Controls** pane, click **Tab**.

3 In the **Settings** pane, type a name for the tab in the **Label** box.

4 Click **OK**.

Remove Controls from the Ribbon

NOTE: You can delete tabs, groups, and individual buttons from the Ribbon. To simplify your workspace temporarily, hide the Ribbon by double-clicking any tab on the Ribbon, or by clicking the **Full Screen** button from the status bar.

To remove a control

1 With a session open in Reflection, select the **Appearance** tab.

2 From the **Menus** group, click the **UI Designer** button to open the **UI Designer**.

3 From the **Design View** pane of **UI Designer**, select the control you want to delete.

4 In the **Arrange Controls** pane, click **Delete.**

5 To view your changes before saving them, in the **Review** pane, click **Preview**.

6 Click **OK**.

Modify Existing Controls on the Ribbon

You can change built-in controls or custom controls.

To modify an existing control

1 On the **Appearance** tab, click **UI Designer**.

2 In the **Design View** pane, from the Ribbon simulation, select the control that you want to modify.

   NOTE: To select a button group, click the bottom edge of the group, or, select one of its buttons, and then, under **Arrange Controls**, click **Select Parent**. To select a group, click the group name.

3 In the **Settings** pane, make your changes.

4 Click **OK**.

Move Controls on the Ribbon

From the **UI Designer,** you can reorganize or simplify your workspace by selecting a new location for the controls.

To move a control within its parent control

◆ To move a control to new location within its parent control (for example, to move a button within a group, or to move a group on a tab), use the **Move** buttons from the **Arrange Controls** pane in the **UI Designer**.

You can move a control from one group to a different group, move a group from one tab to a different tab, or delete a control from its current location and add it to the new location.

To move a control outside its parent control

1 From the **Design View** pane, select the control that you want to move.

2 Write down the settings that appear in the **Settings** pane.

3 From the **Arrange Controls** pane, click **Delete**.

4 Select the tab and group where you want to place the control, or add a new tab and group.

5 From the **Insert Controls** pane:

To insert	Do this
A **Tab**, **Group**, or **Button**	Click the control.
A **Gallery**, **Split Button**, or **Button Group**	Click the control, then from the **Subitems Collector Editor** dialog box, add subitems to the control, and then click **OK**.
A **Built-In**	Click the control, then from the **Built-In Controls** dialog box, choose a pre-defined gallery or group, and then click **Insert**.

6 Change the properties for the control in the **Settings** pane to match the settings you wrote down before you deleted the control from its original location.

7 Click **OK**.

Restore the Default Ribbon

You can reverse any changes you've made to the Ribbon in the **UI Designer** by selecting the default ribbon.

1 With a session open in Reflection, from the **Quick Access Toolbar**, click 📄.

2 Under **User Interface**, click **Manage Ribbon**.

3 Click **Select another Ribbon file**.

4 Click **Built-in** and select a Ribbon from the list that best matches your session document.

5 Click **OK**.

6 To save the session document, on the Quick Access Toolbar, click 📄.

The session will use the Ribbon you selected until you select a different Ribbon.

Import Legacy VT Toolbars to the Ribbon

You can use the UI Designer to import legacy VT toolbars to the Reflection Ribbon. In Ribbon mode, you can import legacy VT toolbars from any legacy VT session file (*.r2w or *.r4w) or toolbar file (*.rtb) to the currently selected VT session. Once imported, the toolbars appear as buttons on the Ribbon.

NOTE: Importing legacy VT toolbar behavior depends on the user interface mode. The Reflection Classic user interface mode automatically imports toolbars for legacy VT sessions. However, when you open a legacy VT session in the Ribbon user interface mode, the session's toolbars are not automatically imported.

In Ribbon Mode, Import Legacy VT Toolbars

1 Open the VT session you want to import the toolbars from and select the session in the workspace.

2 Right click the Ribbon and then select **Customize the Ribbon**.

3 In the Ribbon UI Designer, in the **Insert Controls** group, click **Import**.

4 From the Open dialog box, select the legacy VT session file or the toolbar file you want to import.

UI Designer displays all visible toolbars in the **Convert Legacy Toolbars** panel:
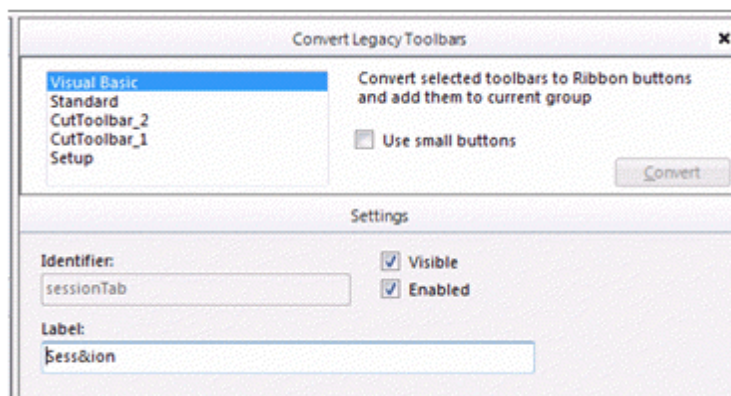
5 Select the Ribbon group you want to import the toolbars to. You can select an existing group or you can add a new tab and a new group.

6 To use small buttons that are grouped vertically in rows of three, select **Use small buttons**.

7 Select the toolbars you want to import and then click **Convert**.

The imported buttons are added to the Ribbon group.

If you checked the "Use small buttons" box, buttons are grouped vertically as follows:
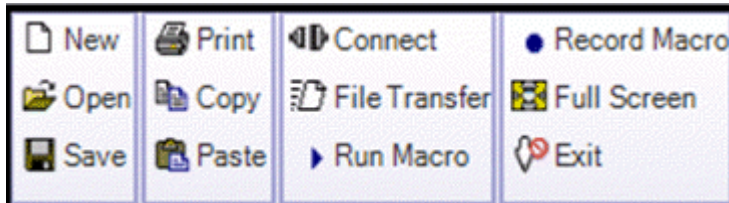
8 Click **OK** and save the .map file.

Minimize the Ribbon

You can hide the Ribbon to provide more working area in the Reflection window.

To hide the Ribbon

1 Click the Quick Access Toolbar menu.

2 In the menu list, choose Minimize the Ribbon.

NOTE: You can display the Ribbon by clicking the Quick Access Toolbar menu button and then choosing Maximize the Ribbon.

If you are using a default 3270 or 5250 keyboard map, you can press CTRL+F1 to hide or display the Ribbon.

Hide Tooltips on the Ribbon, the Status Bar, and the Macro Panel

You can hide the tooltips on the ribbon, the status bar, and the Macro Panel, to make it easier to use the ribbon controls.

To hide the Ribbon

1 Open the Reflection Workspace Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the File menu or the Reflection button ⊕ (if using the Office 2007 Look and Feel), choose **Reflection Workspace Settings**.
Reflection Browser	On the Reflection menu, choose **Settings** and then **Reflection Workspace Settings**.
TouchUx	Tap the Gear icon and then select **Reflection Workspace Settings**.

2 Under **Workspace Settings**, click **Configure User Interface**.

3 Under **UI Preferences**, select **Suppress Tooltips**.

NOTE: The **Suppress Tooltips** setting does not apply to tooltips on dialog boxes or windows such as Screen History.

Customize Classic Menus and Toolbars

You can customize the menus and toolbars used by your Reflection Desktop sessions. You can set up sessions to share the same customized menus and toolbars or you can set up unique menus and toolbars for each session.

After you customize menus and toolbars for a session and save these settings, you can apply them to other sessions.

You can also import toolbars from Reflection 14 or Extra! sessions and then save them in Reflection `.xuml` files that can be applied to other sessions.

In this Topic

- "Create or Modify Menus or Toolbars" on page 110
- "Apply Menu and Toolbar Settings to a Session" on page 110
- "Import Toolbars and Menus into a Session" on page 111

NOTE: For IBM sessions, only Extra! and Reflection Desktop toolbar files can be imported. For VT sessions, Extra!, Reflection Desktop, and Reflection 14 toolbar files can be imported.

Video

▶ How To Customize Menus and Toolbars in Reflection Desktop Classic Mode (3:40)

Create or Modify Menus or Toolbars

To create or modify the Classic menu or toolbar

1 From the Classic user interface mode (page 216), open a session document.

2 Open the Settings window as follows:

    2a For VT sessions, choose **View Settings** on the **Setup** menu.

    2b For other types of sessions, choose **Settings** on the **Options** menu.

3 In the Settings window, under User Interface, choose **Manage Ribbon**.

In Classic sessions, the currently selected ribbon includes "Classic..." in the filename.

4 Choose **Modify the currently selected Ribbon file** or **Create a new Ribbon from an existing Ribbon file**. (When you are using the Classic user interface mode, these Ribbon settings are actually toolbar and menu settings.)

5 If you choose to create a new Ribbon, select an alternate file with "Classic..." to use as your starting point.

NOTE: If you select one of the built-in files that is included in the installation folder, Reflection automatically creates an editable copy of the built-in file and saves the copy with your modifications to the `CustomUI` folder in your Reflection user data folder.

---

6 Use the Classic UI Designer to modify the menu or toolbar items. Changes are saved to the currently selected Ribbon when you click **OK**.

Apply Menu and Toolbar Settings to a Session

You can duplicate toolbars and menus used in other sessions by applying these settings to a session.

To apply menu and toolbar settings to a session

1 From the Classic user interface, open a session document.

2 Open the Settings window as follows:

    2a For VT sessions, choose **View Settings** on the **Setup** menu.

    2b For other types of sessions, choose **Settings** on the **Options** menu.

3 Under **User Interface**, select **Manage Ribbon**.

4 In the Manage Ribbon dialog box, click **Select another Ribbon file** and then select the file you want to apply to the session.

NOTE: After you apply toolbars to a session, you can show or hide the toolbars from a context menu that you open by right clicking on a toolbar area.

Import Toolbars and Menus into a Session

Menus and toolbars associated with Extra! and Reflection 14 sessions are automatically imported when you open and save these sessions. You can also import toolbars from these types of sessions into Reflection Desktop sessions. And you can import other Reflection Desktop toolbars.

NOTE: For IBM sessions, only Extra! and Reflection Desktop toolbar files can be imported. For VT sessions, Extra!, Reflection Desktop, and Reflection 14 toolbar files can be imported.

To import toolbars

1 In the Classic UI Designer Design View panel, select the **Toolbars** tab.

2 Select **Import**.

3 To import toolbars from another Reflection Desktop session, select the toolbar file for that session in the CustomUI folder, under the Reflection user data folder.

4 To import toolbars from Extra! sessions, browse to the folder that contains your toolbars and select the toolbar to import.

5 To import Reflection 14 toolbars, select the session file that includes the toolbars to import or select a Reflection 14 toolbar file.

NOTE: All toolbar and menu settings are saved in Reflection Desktop `.xuml` files.

Set up Workspace Settings

Set up workspace settings that apply to all sessions, including: accessing a Centralized Management Server that you have set up to centrally manage and control sessions, performing a series of actions when the workspace starts, and saving sessions as compound session document files that contain session settings in a single file.

In this Topic

Set up Reflection to Access a Centralized Management Server

Use this procedure to set up Reflection to open session documents that are managed on a centralized management server.

To set up Reflection to use a centralized management server

1 Open the Reflection Workspace Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **File** menu or the Reflection button (if using the Office 2007 Look and Feel), choose **Reflection Workspace Settings**.
Reflection Browser	On the Reflection menu, choose **Settings** and then **Reflection Workspace Settings**.
TouchUx	Tap the Gear icon and then select **Reflection Workspace Settings**.

2 Click **Configure Centralized Management**.

3 In the Configure Centralized Management dialog box, select **Enable Centralized Management**.

4 In Server URL, enter the URL for the centralized management server.

5 Select Test Connection and provide any necessary information to authenticate to the Reflection Management Server.

6 Close and reopen the workspace.

When you reopen the Workspace, any assigned packages are installed and any assigned session profiles are downloaded to your computer. Session profiles are updated if they do not exist or if the "Overwrite end user files" option was selected in the Session Manager.

NOTE: When a session profile is centrally managed it should not be renamed or moved. Doing so will prevent you from receiving updates from the server.

To set up Reflection to access the centralized management server for certificates

1 In the Configure Centralized Management dialog box, select the **Enable certificate management** check box under **Options**.

2 Close and reopen the workspace.

Enable certificate management allows the workspace to access and utilize certificates on a centralized management server. The **Enable Centralized Management** setting must be configured in order to select the **Enable certificate management**check box.

NOTE: For centralized management server configuration information contact your administrator.

Set Up a Workspace Startup Action Sequence

You can set up Reflection to perform a series of actions when a workspace starts, rather than when a session opens and connects to the host.

This allows you to automate actions that are independent of a session. For example, if you are creating Visual Basic for Application (VBA) macros, you can set up an action sequence that opens the VBA Editor and the VBA Guide when you open a workspace.

To set up a workspace startup action sequence

1 Open the Reflection Workspace Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the File menu or the Reflection button ⊕ (if using the Office 2007 Look and Feel), choose **Reflection Workspace Settings**.
Reflection Browser	On the Reflection menu, choose **Settings** and then **Reflection Workspace Settings**.
TouchUx	Tap the Gear icon and then select **Reflection Workspace Settings**.

2 Under **Workspace Settings**, click **Configure Workspace Defaults**.

3 Under **Workspace and Documents**, in the **When starting workspace** list, select **Run Startup action**.

4 Click **Select Action**.

5 On the left pane of the Select Action dialog box, under **Map To,** select **Action Sequence**.

6 Click **Add** and then, in the **Action** list, choose an action.

7 Repeat Step 6 to add additional actions and complete the action sequence.

NOTE: You can also add actions to the list by selecting an action and then clicking **Duplicate**.

Stop Showing the Create New Document Dialog Box

By default, the **Create New Document** dialog box is displayed when you open the Reflection workspace.

To stop showing the Create New Document dialog box

1 Open the Reflection Workspace Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the File menu or the Reflection button (if using the Office 2007 Look and Feel), choose **Reflection Workspace Settings**.
Reflection Browser	On the Reflection menu, choose **Settings** and then **Reflection Workspace Settings**.
TouchUx	Tap the Gear icon and then select **Reflection Workspace Settings**.

2 Under Workspace Settings, click **Configure Workspace Defaults**.

3 In the **When starting workspace** box, select **Show nothing**.

Related Topics

• "Create New Document Dialog Box" on page 218

Choose Whether to Participate in the Product Experience Improvement Program

The Product Experience Improvement program is designed to help Micro Focus improve Reflection over time. This program collects information about how people use Reflection without interrupting the users in their tasks. The information that is collected helps Micro Focus identify which Reflection features to improve.

NOTE: For a detailed list of the types of information this program gathers, see "Configure Usage Data Dialog Box" on page 228.

Reflection is set to participate in this program by default. If you choose not to participate, you'll need to clear the **Enable Usage Data** Option as follows.

To choose whether to allow Reflection to gather usage data

1 Open the Reflection Workspace Settings dialog box.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the File menu or the Reflection button ⚙ (if using the Office 2007 Look and Feel), choose **Reflection Workspace Settings**.
Reflection Browser	On the Reflection menu, choose **Settings** and then **Reflection Workspace Settings**.
TouchUx	Tap the Gear icon and then select **Reflection Workspace Settings**.

2 Under **Workspace Settings**, click **Configure Usage Data**.

3 Select whether to participate in the Product Experience Improvement program by selecting or clearing the **Enable Usage Data** option.

4 Close and reopen the workspace.

NOTE: This setting is saved in the `Application.Settings` file. If you are deploying this setting, you will need to create a package for this custom file as shown in "Configure And Automatically Package Workspace Settings" in the Reflection Deployment Guide.

Save Reflection Sessions as Compound Session Document files.

You can set up Reflection to save session document files as compound session files when sessions are saved (using the Save menu). These files include all of the customized settings for QuickPads, keyboard maps, themes, mouse maps, hotspots, and ribbons. By default, this configuration data is saved in separate files that must be deployed to specific folders.

To set up Reflection to save sessions in compound files

1 Open the Reflection Workspace Settings dialog box.

   The steps depend on your user interface mode:

User Interface Mode	Steps
Ribbon	On the **File** menu or the Reflection button ⚙ (if using the Office 2007 Look and Feel), choose **Reflection Workspace Settings**.
Reflection Browser	On the Reflection menu, choose **Settings** and then **Reflection Workspace Settings**.
TouchUx	Tap the Gear icon and then select **Reflection Workspace Settings**.

2 Click **Configure Workspace Defaults**.

3 Under Workspace, select **Save session as compound document**.

When you save a document, it is saved in a compound session document file.

Perform Other Common Tasks

You can perform these common tasks to make it easier to use Reflection or configure it to meet your requirements.

In this Topic

- Broadcast Commands to Multiple VT Sessions
- Capture Incoming Screen Data (VT)
- Add a Keyboard Shortcut That Sends Special Character Data (VT)
- Edit the Translation Table
- Use Customized Host Files
- Generate a HLLAPI Trace

Broadcast Commands to Multiple VT Sessions

If you manage multiple host machines, you may often need to send the same command to more than one host and reentering the command on each host can be tedious. You can save time by using the CommandCast feature to broadcast the commands you enter in one host to any number of other hosts that you have selected to receive the commands.

NOTE: CommandCast is supported only for VT sessions. You can use this feature for sessions you open in all user interface modes except the **Classic** user interface mode.

To broadcast commands from a VT session to other VT sessions

1 In Reflection Desktop, open the VT session in which you want to enter the commands and the sessions you want to send commands to.

2 Open the **CommandCast** Panel as follows:

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Tools** tab, in the **Tools** group, click the **CommandCast Panel** button.
Classic MDI	On the toolbar, click the CommandCast button 📢 .

3 In the **CommandCast Panel**, click the sessions you want to include in the broadcast.

The **CommandCast Panel** displays a list of open VT sessions. It shows which session is set to broadcast commands, and which sessions are set to receive them. The last session you click is the session you broadcast from.
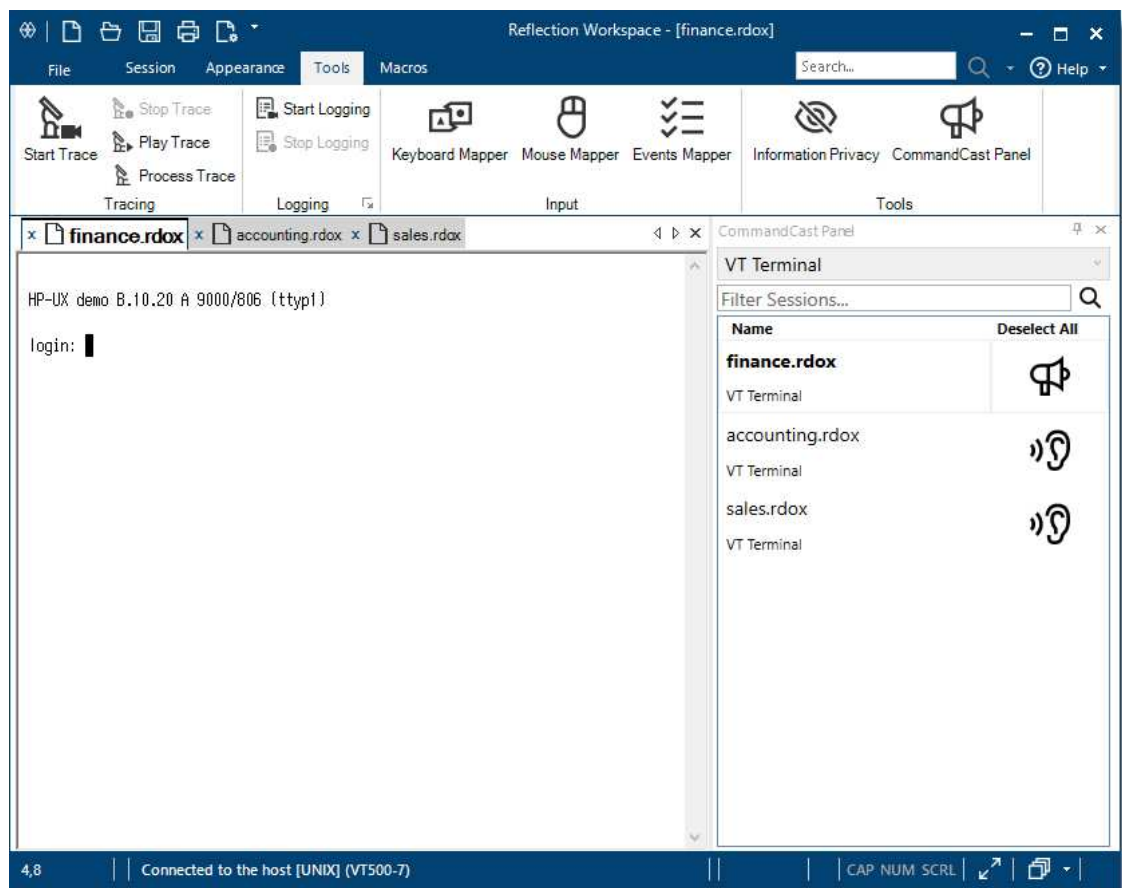
4 To broadcast from another session, select the session in the workspace window or click that session in the **CommandCast** panel.

5 If you want to be able to see the commands you enter and their output on each of the servers, click [icon] on the status bar and select **Tile Vertical**.
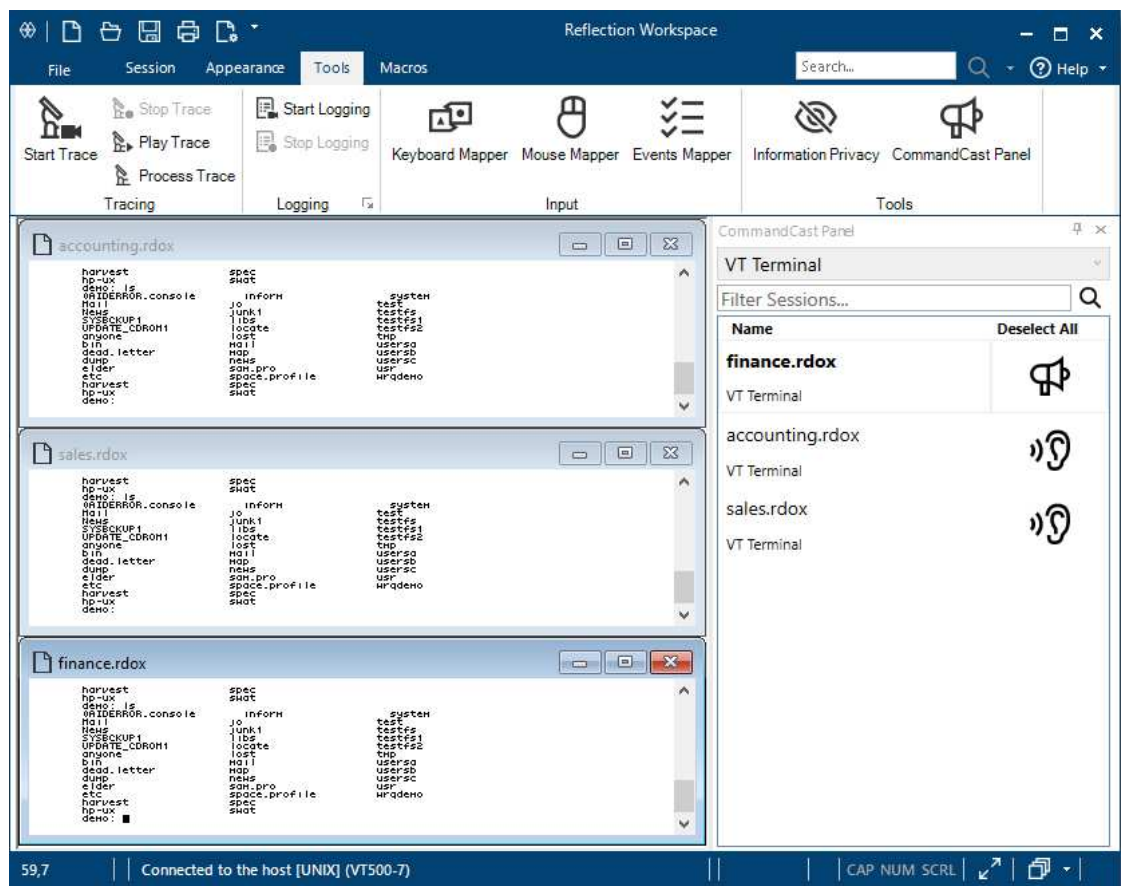
6 Enter the command you want to broadcast.

The command you enter and the resulting output are displayed on all the host machines you are broadcasting to.

7 If you routinely broadcast to this group of hosts, select **Save Layout** on the **File** menu to save this group as a layout.

The **CommandCast Panel** settings are saved with the layout. The next time you want to broadcast to these hosts, you can open the layout to open all the sessions, along with your previous **CommandCast Panel** settings.

Capture Incoming Screen Data (VT)

You can use the **Capture Incoming Data** action to capture data received from the host and save it to a file. This allows you to save a report (or other data) on the host screen and distribute it as a text file. It is also useful for logging data received from the host.

Using the Capture Incoming Screen Data action has advantages over printing or tracing data. Unlike when you print data to a file or create a trace file, captured lines are not wrapped, and you can choose whether to capture all of the data (including control sequences) or text data only.

Capture incoming data in Classic mode

If you are using a Classic interface mode, you'll need to make sure your session compatibility is set for Extra! as follows.

To capture incoming data in Classic mode

1 From the **File** menu, select **New Session** to create a new session document.

2 In the Create New Document dialog box, select **VT Terminal** and then in the **Compatibility** list (at the bottom of this dialog box), select **Extra!**.

3 To capture data from the host, on the **Tools** menu, select **Capture Incoming Data**.

4 In the Capture Incoming Data dialog box, browse to the file you want to save the data in and select whether to append the data you capture to an existing file or overwrite the file each time you start capturing data.

5 If you want to omit control sequences from the captured data, select **Save As Text**.

   All of the data sent by the host is saved to the file you specified.

6 When you want to stop capturing data, on the **Tools** menu, select **End Capture**.

Capture incoming data in Ribbon mode

If you are using the Ribbon mode interface, you'll need to map the **Capture Incoming Data** action to a button on the Ribbon interface as follows.

To capture incoming data in Ribbon mode

1 Click the Quick Access Toolbar menu, and then select **Add an Action**.

2 In the Select Action dialog box, in the Action list, select **Capture Incoming Data**.

3 In the Capture Incoming Data dialog box, browse to the file you want to save the data in and select whether to append the data you capture to an existing file or overwrite the file each time you start capturing data.

4 If you want to omit control sequences from the captured data, select **Save As Text**.

5 To capture data from the host, select 🔲 on the Quick Access Toolbar.

   All of the data sent by the host is saved to the file you specified.

6 When you want to stop capturing data, select ⊗ on the Quick Access Toolbar.

Add a Keyboard Shortcut That Sends Special Character Data (VT)

You can add an action that sends special characters to the host and then map it to a keyboard shortcut, a button, or another control.

To add a keyboard shortcut that sends special character data to the host

1 Open the Document Settings dialog box.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ⬚.
TouchUx	Tap the Gear icon and then select ⬚ **Document Settings**.

2 Select **Manage Keyboard Map**.

3 In the Keyboard map dialog box, select **Modify the currently selected keyboard map file**.

4 Press the key combination you want to map (for example, `CTRL+Q`).

5 Click **Select Action** and then select the **Send Text** action.

6 In the **Select a special character** list, choose the character data to send.

NOTE: If the **Select a special character** list doesn't have the character data you want to send, you can type in the string for the character data in the **Text to send to host** field. For example, type in `<ESC>`. Alternatively, you can hold down the ALT key and use the numeric keypad to enter the numeric code for the data. For example, to send `<ESC>`, enter `027`.

Edit the Translation Table

Using the Translation Tables dialog box, you can:

- Edit the tables Reflection uses to translate the PC's character set into the character set used by the host and vice versa.
- Use currently unsupported character sets.
- Customize Reflection for unique host environments.

Use the translation tables when:

- You need to edit how characters are translated from the host to the PC, and vice versa. Typically, you'll use the tables to support a host character set that's currently unavailable in Reflection. The characters in the table are hexadecimal.

  - or -

- You need to edit how EBCDIC characters are translated from the host to the PC, and vice versa for a Unisys T27 host. These translations are done in addition to the normal PC-to-host and host-to-PC translations performed by Reflection. The characters in the table are hexadecimal.

NOTE: To use the translation tables, the `DataStreamTranslation` VBA property must be set to `true`(the default is `false`). When Reflection is emulating a Unisys T27 host, the `DataStreamTranslation`property is automatically set to true.

To open the Translation Tables dialog box

1 Launch a Reflection VT session.

2 From the Tools ribbon, select **Visual Basic**.

3 In the VBA editor, right-click on **Project Legacy** and choose **Insert** and then **Module**.

4 Copy and paste the following VBA code into the code window:

```
Sub Translation()
     With Session
     .DataStreamTranslation = True
     .ExecuteBuiltInFunction "TranslationTables"
     End With
End Sub
```

5 Close the VBA editor.

6 On the Tools ribbon, click **Run Macro**.

7 In the Run Macro dialog box, select **Legacy Reflection Macro in This File**.

8 Run the `Translation`Macro.

   The Translation Tables editor is displayed.

Use Customized Host Files

Reflection supports legacy Reflection custom host files. These files are used to specify the host names displayed in the **Host name/IP address** list in the Settings dialog box.

The path to the customized host file is specified in the value for the `HKCU\Sofware\WRQReflection\Rwin\Global` registry setting. This registry setting is only installed in legacy versions of Reflection. It is not part of the Reflection installation.

If the value of this setting is "" (the default) or if the setting is not in the registry, all of the names in the system local host file are displayed in the Host name/IP address list.

NOTE: Windows can resolve the host names in the custom host files only if these names are valid domain names or names that are in the local hosts file. Custom host files are not used by Windows to resolve IP addresses.

Host file format

The custom host file must have the following format:

`<IPv4 or IPv6 address> <host name>`

For Example:

```
127.0.0.1 localhost
:: localhost
```

The host name information is used to populate the **Host name/IP address** list in the Settings dialog box.

The IP address information is not relevant unless the specified host file also happens to be the Windows system hosts file.

Generate a HLLAPI Trace

HLLAPI is a standard API for automating terminal tasks. A HLLAPI trace displays the HLLAPI calls the application is making, including return codes. You can use the trace for troubleshooting problems with a HLLAPI application and send the generated file to customer support.

To create a HLLAPI trace

1 In the Reflection Workspace Settings dialog box, select **Configure Workspace Attributes**. Then select **Enable HLLAPI logging** and specify a HLLAPI log file name in a location where you have the appropriate permissions to create and save a file.

2 In the Reflection Workspace, open or create a session document to connect to your IBM host, and start the HLLAPI application. Perform the actions you want to record in the trace.

3 Close the HLLAPI application.

   The trace file is automatically saved as `hllapi.log` in the folder selected in the HLLAPI log file box.

Print

You can print screen data on Windows printers. You can print a list of screens and then specify how many screens to print on a page or set up Reflection to print multiple screens as a continuous flow of text, without page breaks at the beginning or end of screens.

In this Topic

Print More Than One Screen per Page

You can capture and then print multiple screens on each page in two different ways.

◆ You can capture a list of screens and then specify how many screens to print on a page.

   Or

◆ You can set up Reflection to print multiple screens as a continuous flow of text, without page breaks at the beginning or end of screens.

To capture a list of screens and specify how many to print on a page

1 Open the Print Multiple Screens pane.

The steps depend on your user interface mode.

- If you are using the Ribbon mode, from the **File** menu, choose **Print** and then choose **Print Multiple Screens**.

- If you are using Classic mode, from the **File** menu, choose **Print Multiple Screens**.

2 In the **Print Multiple Screens** pane, click the Capture Screen button ⬜ to select the screens you want to print as you navigate through your application.

3 Select the number of screens to print on a page.

4 When you are ready to print all of the screens, click the Print Screens button 🖶 on the **Print Multiple Screens** pane.

CAUTION: Do not close the **Print Multiple Screens** pane until you have finished printing the screens. When you close this pane, the screens you captured are discarded.

To print multiple screens as a continuous flow of text

You can set up Reflection to print multiple screens so that the screen information is printed in a continuous flow across the pages, without page breaks at the start or end of each screen.

NOTE: If you prefer not to flow information for individual screens across pages, you can choose to insert a form feed between screens to force page breaks.

---

1 Open the Print dialog box.

The steps depend on your user interface mode (page 216).

- If you are using the Ribbon or Browser mode, click 🖶 on the Quick Access Toolbar. Then, in the Print dialog box, click **Setup**.

- If you are using Classic mode, from the File menu, choose **Print Settings** or **Print Setup**

2 At the bottom of the Print Setup dialog box, in the **Multiple screens per page** box, select **Close printer manually**.

3 If you want Reflection to add a form feed to force a page break between each screen, select **Auto formfeed**.

4 For each screen you want to print, go to the screen, and then, on the toolbar, click the 🖶 Print button.

After you print the first screen, the **Close Printer** button appears on the status bar.

NOTE: Each screen you send to the printer is spooled to a file until you click **Close Printer**.

---

5 When you are done selecting the screens to print, click **Close Printer**.

The screens are printed.

Set Up a Default Windows Printer

You can specify which Windows printer to use for the session.

To set up printing

1 Open the Document Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ⬚.
TouchUx	Tap the Gear icon and then select ⬚ **Document Settings**.

2 Under **Printer Settings**, select **Configure Printer Settings**.

3 On the Print Setup dialog box, select the printer to use.

Transfer Files

You can transfer files using mainframe file transfer or FTP file transfer.

In this Topic

Transfer IBM mainframe files

You can send or receive files on IBM3270 mainframes or IBM System i systems.

To transfer files to a mainframe from your PC

1 Connect and log on to the mainframe.

The **File Transfer** button on the ribbon (or the **Transfer File** menu item if you are using Classic interface mode) is available only after you connect.

2 Open the File Transfer dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
The Reflection Ribbon	On the **Session** tab, from the **Transfer** group, click ⬆ **File Transfer**.
Classic or Classic MDI	On the Tools menu, choose **Transfer File**.
The Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**.

3 Click the **Settings** button, and configure the file transfer settings.

For most situations, you can configure for file transfers by selecting a preset configuration in the **Protocol** tab.

4 Click **OK**.

5 From the **Transfer** dialog box, under **Local,** do one of the following:

- ◆ Browse under **Local folders**, and then select one or more files from the list.

   -or-

- ◆ Type the path and filename into the **File names** box.

6 Select your preferences for **Transfer method**, **If file exists**, and **Record format**.

7 Specify the host file information:

For this host system	Do this
CICS	Type a filename in the **File names** box.
	It is not possible to perform transfers involving multiple files.
	If you don't type a filename, Reflection uses the PC filename, with the period and extension, if applicable, removed. To avoid overwriting files, do not send files with the same filename and different extensions.
CMS	Click **Show host files**, and browse to select one or more host files.
	-or-
	Type the file information into the **File names** box.
	If you don't type a filename, Reflection uses the PC filename. If a PC file you are transferring does not have a file extension, the transfer fails.
TSO	Click **Show host files**, and browse to select one or more host files.
	All datasets that have a high-level qualifier that equals your user ID are displayed.
	-or-
	Type the file information into the **File names** box.
	If you don't type a filename, Reflection uses the PC filename.

8 To initiate a file transfer, do one of the following:

- ◆ Click the ⬚▸ **Transfer** button.

    -or-

- ◆ Drag the source file, and then drop it on the desired destination file

To transfer files from a mainframe to the PC

1 Open the Transfer dialog box.

   1a Start Reflection and log on to the host computer as usual.

   1b The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
The Reflection Ribbon	On the **Session** tab, from the **Transfer**group, click **File Transfer**.
The Reflection Browser	On the Reflection menu, choose **Tools**and then **File Transfer**.
TouchUx	Tap the Wrench icon and then under **Tools**, select **File Transfer**.

2 Click the **Settings** button, and configure the file transfer settings.

For most situations, you can configure for file transfers by selecting a preset configuration in the **Protocol** tab.

3 Click **OK**.

4 Specify a host file:

For this host system	Do this
CICS	Type a filename in the **File names** box.
	It is not possible to perform transfers involving multiple files.
CMS	Click **Show host files**, and browse to select one or more host files.
	To filter the list, you can enter partial filenames or wildcards; for example, to see all files that begin with the letter "d" of the mode "files" on the "a" disk, type the following:
	`d* files a`
	-or-
	Type the file information into the **File names** box.
TSO	Click **Show host files**, and browse to select one or more host files.
	All datasets that have a high-level qualifier that equals your user ID are displayed.
	-or-
	Type the file information into the **File names** box.

5 Select your preferences for **Transfer method**, **If file exists**, and **Record format**.

6 From the **Transfer** dialog box, under **Local,** do one of the following:

- ◆ Browse under **Local folders**, and then select one or more files from the list.

 -or-

- ◆ Type the path and filename into the **File names** box.

 If you omit this step, Reflection uses the host filename.

7 To initiate a file transfer, do one of the following:

- ◆ Click a **Transfer** button to move the file in the indicated direction.

 -or-

- ◆ Drag the source file, and then drop it on the desired destination file.

See	For information about...
"IBM System i (AS/400) Transfer" on page 681	IBM System i (AS/400) transfer configuration options
"Batch Transfers" on page 719	Creating a list of transfers in a transfer request file that can be used to perform multiple transfers in a single operation
"Configure File Transfer" on page 684	Configuring file transfer settings
"Saving and Repeating Transfers" on page 717	Transfer request files
"IBM File and Data Transfer" on page 669	Support for IBM file transfer
"Use File Transfer Naming Templates" on page 674	How to set up a file transfer template to define a set of conditions that affects the way Reflection names files transferred between your PC and a host
"Mainframe File Transfer" on page 670	Mainframe file transfer
"Create a File Transfer Template" on page 675	How to create a custom file template
"Transfer Request Files" on page 717	Creating a transfer request file so you can perform the same transfer (or transfers) again later, without having to specify files and options each time.

Transfer Data to or From an IBM System i (AS/400)

NOTE: If you plan to perform a transfer regularly, you can save your transfer settings in a transfer request file.

To send data to a member of a file on an IBM System i (AS/400)

1 In a 5250 session, open the File Transfer dialog box.

 The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
The Reflection Ribbon	On the **Session** tab, from the **Transfer** group, click **File Transfer**.
Classic or Classic MDI	On the Tools menu, choose **Transfer File**.
The Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**.

2 Click the **Settings** button to open the Transfer Settings dialog box.

3 On the **AS/400** tab, specify the host to send the data to and the credentials (Username and Password) you want to use to log on to the host.

> **NOTE:** You can transfer data to a host other than the host your session is connected to.

4 On the **Options** tab, under **To host**, browse to the Description `.FDF` file that was created when you downloaded the file from the host. (Reflection creates this file by default when you download a file.)

5 In the **Objects** list, select one of the options to create a new member or replace an existing member.

6 If you are creating a new member in a file, enter a description in the **Member text** box. (This step is optional.) This text description is displayed when you view the files in your application.

7 On the **Translation** tab, specify how to handle filename spaces, underscores, length, and case and click **OK**.

8 From the **Transfer** dialog box, under **Local,** do one of the following:

- Browse under **Local folders**, and then select one or more files from the list.

  -or-

- Type the path and filename into the **File names** box.

> **NOTE:** You can transfer more than one file only if the description `.FDF` file you are using applies to all the files.

9 Under **Host**, specify which host file and member should receive the data using one of the following techniques:

- To create a member, click **Show Host Files** and browse to select a host file or type the file information in the **File names** box, using this syntax: `LIBRARY/FILE`

  -or-

- To replace a member, click **Show Host Files** and browse to select a host file and member or type the file information in the **File names** box, using this syntax: `LIBRARY/ FILE(MEMBER)`

> **NOTE:** If Reflection is configured to use a character set that is not supported by your host, you cannot display host files using the **Show host files** button.

10 To initiate a file transfer, do one of the following:

- Click the [image] **Transfer** button.

-or-

 ◆ Drag the source file, and then drop it on a destination file.

To send data to a new file and member on an IBM System i (AS/400)

1 In a 5250 session, open the File Transfer dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
The Reflection Ribbon	On the **Session** tab, from the **Transfer** group, click **File Transfer**.
Classic or Classic MDI	On the Tools menu, choose **Transfer File**.
The Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**.

2 Click the **Settings** button to open the Transfer Settings dialog box.

3 On the **AS/400** tab, specify the host to send the data to and the credentials (Username and Password) you want to use to log on to the host.

> **NOTE:** You can transfer data to a host other than the host your session is connected to.

4 On the **Options** tab, under **To host**, browse to the Description .FDF file that applies to the file you are transferring. (Reflection creates this file by default when you download a file.)

5 To create a new file and member, in the **Objects** list, select **Create File and Member** and then enter the following settings:

 ◆ In **File type**, select the type of file to create (**Data** or **Source**).

 ◆ In the **Authority** list, choose the type of file permissions (for example, **Read/Write)** for the file.

 ◆ To add a description for the file, enter a description in the **File text** box. (This is optional.) The text description is displayed when you view the files in your application.

 ◆ To add a description for the member, enter a description in the **Member text** box. (This is optional.) The text description is displayed when you view file members in your application.

 ◆ In the **Reference file** box, specify a reference file to use for the file you are sending, using the following syntax:

```
library_name/filename
```

The new host file is created using the field names in the description file and the definitions of the fields in the reference file.

> **NOTE:** A reference file is a physical file that defines the fields used in other files. You can create a field reference file that contains only the field descriptions that you need for any group of files or you can specify a file that has the same fields as the file you are creating.

6 On the **Translation** tab, specify how to handle filename spaces, underscores, length, and case and click **OK**.

7 From the **Transfer** dialog box, under **Local,** enter the file you want to transfer:

 ◆ Browse under **Local folders**, and then select the file from the list.

-or-

 ◆ Type the path and filename into the **File names** box.

8 Under **Host**, enter the library and the new host file in the **File names** box, using this syntax:

`LIBRARY/FILE(member)`

NOTE: If Reflection is configured to use a character set that is not supported by your host, you cannot display host files using the **Show host files** button.

---

9 To initiate a file transfer, do one of the following:

 ◆ Click the ⬚▸ **Transfer** button.

 -or-

 ◆ Drag the source file, and then drop it on a host library.

To receive data from an IBM System i (AS/400)

1 Open the File Transfer dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
The Reflection Ribbon	On the **Session** tab, from the **Transfer** group, click **File Transfer**.
Classic or Classic MDI	On the Tools menu, choose **Transfer File**.
The Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**.

2 Click the **Settings** button, and configure the file transfer settings.

3 On the **AS/400** tab, specify the host to receive the data from and the credentials (**Username** and **Password**) you want to use to log on to the host.

NOTE: You can transfer data from a host other than the one your session is connected to.

---

4 On the **Options** tab, under **From host**, specify how you want Reflection to handle AS/400 transfers and select one of the following options in the **Output to** list.

Choose this option	To...
Display	Display the file in the Query Results display window.
File	Send the data to a file.
	If you don't specify a filename, Reflection uses the host filename.
Spreadsheet	Save the file in a DIF file that can be opened in a spreadsheet.

5 If you are transferring files to the `BIFF` or `BIFF8` file format and you want to include the column labels in your transfer, select **Save column header (BIFF and BIFF8 only)**.

6 On the **Translation** tab, specify how to handle filename spaces, underscores, length, and case and click **OK**.

7 (Optional) To configure an SQL query, click **Settings** and from the **SQL** tab, build your query.

Field information about the host file you selected is available when you click an arrow `>` next to a field.

8 In the **Transfer** dialog box, under **Host**, specify the host file from which to receive data as follows:

- Click **Show host files**, and browse to select one or more host files. If the library containing the host file you need is not shown, click **Add library** and type the library name in the **Add Library** dialog box.

  -or-

- Type the file information using this syntax: `LIBRARY/FILE(MEMBER)`.

  NOTE: If Reflection is configured to use a character set that is not supported by your host, you cannot display host files using the **Show host files** button.

9 In the **Transfer method** list, select how data conversion should be handled. For example, to transfer to a `BIFF` format, select **BIFF** or **BIFF8**.

10 If you chose to transfer the data to a file, choose the file to receive the data under **Local**, in the **File names** box.

- If you chose to output to a file on the **Options** tab, enter the file name and extension. (For BIFF or BIFF8 file transfers, use an `.xls` file extension. For example, use `data.xls`)

- If you don't choose a file, the file is saved with the name of the file on the host.

  NOTE: If you chose to output to a spreadsheet on the Transfer Settings options tab, the file is automatically transferred as a `DIF` file.

11 To initiate a file transfer, do one of the following:

- Click the **Transfer** button.

  -or-

- Drag the source file, and then drop it on the destination file.

Related Topics

- "IBM System i (AS/400) Field Description Files" on page 681
- "Transfer Dialog Box" on page 715
- "Transfer Settings Dialog Box" on page 685
- "IBM System i (AS/400) Transfer" on page 681

Transfer Files To and From HP3000, UNIX, and VMS Systems

Use Reflection to transfer files between your PC and an HP 3000 (including Classic, MPE/iX, and POSIX), VMS (including OpenVMS and Alpha computers), ULTRIX, Unisys, Linux Console or UNIX system. Or, transfer files to any host or electronic service that supports the FTP, Zmodem, Xmodem, Kermit, or SuperKermit protocols.

Reflection includes its own proprietary protocol, called the WRQ/Reflection protocol. Before you can transfer a file for the first time, your administrator must upload the host file transfer program. Host programs are provided for HP 3000, VAX/VMS (DEC), AXP machines, and UNIX operating systems. A system administrator may have already uploaded the host program; if so, you can skip this step.

To transfer a file

1 Open the File Transfer dialog box.

   1a Start Reflection and log on to the host computer as usual.

   1b The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
The Reflection Ribbon	On the **Session** tab, from the **Transfer**group, click **File Transfer**.
The Reflection Browser	On the Reflection menu, choose **Tools**and then **File Transfer**.
TouchUx	Tap the Wrench icon and then under **Tools**, select **File Transfer**.

2 From the **Transfer** dialog box, select a **Protocol**.

3 Select a **Transfer type**.

4 Select the action you want to occur if the transferred file exists in the target location.

   For more information about the options available, see the "Transferring Existing Files" on page 727 topic.

5 Click the **Settings** button, and configure the file transfer settings.

   For most situations, you can configure for file transfers by selecting a preset configuration in the **Protocol** tab.

6 Click **OK**.

7 Perform the file transfer using one of the following methods:

   ◆ Drag one or more files directly from Windows Explorer to the Host icon in the **Transfer** dialog box (or from the **Host file names** list to Windows Explorer).

   -or-

   ◆ Drag one or more files between the **Local** and **Host** boxes in the **Transfer** dialog box.

   -or-

   ◆ Type one or more filename(s) in the text boxes, and then click one of the **Transfer** buttons.

   For more information about the filenaming options available, see the "Filenaming and Wildcards" on page 732 topic.

When the transfer begins, the **File Transfer in Progress** window opens. When transferring multiple files, this window displays the name of each file as it is being transferred; when the **If file exists** option is set to **Cancel** or there is some other error that stops the transfer, any remaining files matching a wildcard specification are not transferred. To cancel a file transfer in progress, click the **Cancel** button, press ESC, or press SPACEBAR.

For more, see the following topics:

See	For additional information about...
"VT File Transfer" on page 723	Transferring files in HP3000, UNIX, and VMS systems.
Transfer Protocols	Supported file transfer protocols.
Transfer Types	The ASCII, Binary, and Image file types and the Auto-detect option.
"Transferring Existing Files" on page 727	How to handle local or host file transfers when a file already exists at the file transfer destination
"Transfer a File with Kermit" on page 730	How to transfer files between a PC and a host running Kermit protocol.

Transfer Files with FTP

You can transfer files in the FTP Client with a simple drag and drop operation. You can drag individual files, multiple files, and entire folders.

To transfer files with FTP Client

1 Connect to an FTP site.

2 Specify a transfer method (**Tools** > **Transfer Method**).

3 Set the preference for handling existing files. (**Tools** > **If File Exists**).

NOTE: Additional file transfer settings are available from the *Site* > **Properties** dialog box. You can use these site-specific properties to configure file transfer.

---

4 Browse to locate the files or folders you want to transfer and the destination location.

5 Select the files or folders you want to transfer and drag them from the source location to your desired destination.

See	For additional information about...
"Transfer Files between Two Remote Sites" on page 808	How to use the FTP Client to drag files between two remote sites
"FTP Client Troubleshooting" on page 828	How to troubleshoot problems such as site-to-site transfer, client connections, and file transfer problems.
"Using the FTP Command Window" on page 838	FTP and SFTP command syntax.
"Resume an Incomplete Server File Download" on page 810	How to resume an incomplete download of a server file to your PC
"Options for Automating FTP Client Transfers" on page 774	Information about using FTP client scripts and the FTP Client Automation API.

See	For additional information about...
"Set the Transfer File Type (Transfer Method)" on page 805	Set the file type (ASCII, binary, Tenex, or Smart) for transfers
"Connecting to an FTP or SFTP Server" on page 774	Connecting to a site, preserving a connection to a server, and making secure FTP client connections
"FTP Scripting" on page 841	FTP client scripting and script file format
"Command Reference" on page 848	FTP and SFTP commands

Configure non-FTP File Transfer

You can manually configure file transfer settings in the Transfer Settings dialog box. Any configuration you perform is saved with your session document.

However, using an automated preset configuration is recommended.

To configure file transfer

1 Open a terminal session.

2 Open the Transfer Settings dialog box.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Session** ribbon, from the **Transfer** group, click the **Transfer Settings** launcher:
Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**. In the Transfer dialog box, click the **Settings** button.
TouchUx	Tap the Wrench icon and then under **Tools**, select **File Transfer**. In the Transfer dialog box, click the **Settings** button.

3 Configure the file transfer settings.

4 For most situations, you can configure for file transfers by selecting a preset configuration in the **Protocol** tab (For example, AS/400).

4 The User Interface

With Reflection Desktop, you can display sessions in five types of user interface modes: Ribbon, Browser, TouchUx, Classic, and Classic MDI.

- "Configuring Reflection" on page 140
- "Using Layouts" on page 141
- "Search" on page 143
- "Customize Ribbons, Menu, and Toolbars" on page 147
- "The User Interface" on page 216
- "Create New Document Dialog Box" on page 218
- "Change the UI Language" on page 219
- "Reflection Workspace Settings Dialog Box" on page 219
- "Configure Workspace Defaults Dialog Box" on page 221
- "Configure Workspace Attributes Dialog Box" on page 223
- "Configure User Interface Dialog Box" on page 224
- "Configure Centralized Management Dialog Box" on page 227
- "Configure Usage Data Dialog Box" on page 228
- "Manage On-Screen Keyboard Settings" on page 229
- "Manage Themes Dialog Box" on page 229
- "Select a Theme File Dialog Box" on page 230
- "Modify Theme Dialog Box (3270 Terminal Sessions)" on page 231
- "Modify Theme Dialog Box (5250 Terminal Sessions)" on page 233
- "Modify Theme Dialog Box (VT Terminal Sessions)" on page 235
- "Manage Themes Dialog Box (6530 Sessions)" on page 237
- "QuickPads" on page 239
- "Workspace Settings Dialog Box" on page 241
- "CommandCast Panel" on page 242

Video

The Reflection Ribbon (2:48)

Using the Reflection Browser (3:11)

The User Interface Options

The Ribbon

The Ribbon interface shares the look and feel of Microsoft Office. In the area between the Quick Access toolbar (the toolbar in the upper-left corner) and the document window is the Ribbon, a dynamic, collapsible device that organizes commands, buttons, and other controls on tabs for each task area. Double-click any tab in the Ribbon to hide or show the Ribbon. Or, if you prefer, you can map a keyboard shortcut to show or hide the Ribbon with a keystroke.Sessions using the default 3270 or 5250 keyboard map already have this action mapped to CTRL+F1.

The Browser

The Browser interface has a look and feel that is similar to the latest Web browsers. You can access commands from the Reflection menu or from the Quick Access Toolbar. You can also access commands by searching for them in the search box and then clicking on the search results.

TouchUx

The TouchUx interface provides the Reflection TouchUx user experience. Reflection runs on Microsoft Windows devices or other devices (Apple iPad or Android) that are accessing sessions running on a Citrix server. This mode includes an on-screen terminal keyboard that can be set as a transparent overlay or docked in a separate pane.

Classic

A Classic interface option provides an interface that is familiar to users of previous versions of Reflection. When using the Classic UI, only one document can be open in a workspace, and other features may not be available.

Classic MDI

The Classic MDI option is similar to the Classic option. Unlike Classic, it provides a multi-document interface that allows more than one document to be open in a workspace.

To select the interface type

1 Open the Reflection Workspace Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **File** menu or the Reflection button (if using the Office 2007 Look and Feel), choose **Reflection Workspace Settings**.
Reflection Browser	On the Reflection menu, choose **Settings** and then **Reflection Workspace Settings**.
TouchUx	Tap the Gear icon and then select **Reflection Workspace Settings**.

2 Click **Configure User Interface** to open the User Interface dialog box.

3 In the **User interface mode** list, select the type of interface that you want to use.

4 To select a look and feel for the Ribbon or TouchUx interfaces, choose from the options in the **Look and Feel / Color scheme** list.

5 Close and reopen the workspace

Workspace and Layouts

Most of your work in Reflection will be done in the application frame, which is called the *workspace*.

You can configure your workspace with several different types of "look and feel" settings that provide different ways to access the workspace menu, which contains layout options, application and document settings, and a list of recent documents.

The Steps to open your workspace settings dialog box depend on your User Interface Mode.

User Interface Mode	Steps
Ribbon	On the **File** menu or the Reflection button (if using the Office 2007 Look and Feel), choose **Reflection Workspace Settings**.
Reflection Browser	On the Reflection menu, choose **Settings** and then **Reflection Workspace Settings**.
TouchUx	Tap the Gear icon and then select **Reflection Workspace Settings**.

The workspace incorporates these elements:

Quick Access toolbar	From this toolbar, located in the upper-left corner, you can perform common tasks and access document settings.

Search	Search the current document, or use the associated drop-down menu to search all open documents, screen history, your desktop, the Reflection Help system, or the Web.
	From other locations in the product, you can also search settings pages, the Help system, or the Micro Focus Support site.
	When using the Reflection Browser, you can also search for commands (for example, Trace), and then choose a command from the search results. (In other words, you can use the search results like a menu.)
Help	When using the Ribbon, click this button, located to the right of the Search box, to open the Reflection Help system, or use the associated drop-down menu to access VBA or API documentation, or to launch the Micro Focus Support site.
	When using the Reflection Browser, access the Help from the **Reflection** menu.
Document window	The document window is the area in which your terminal sessions or Web pages are displayed.
	You can increase the size of the document window by hiding the Ribbon or by choosing Full Screen mode. In Full Screen mode, Reflection expands the document window to fill your entire screen, creating more space in which to display your documents.
	Documents in the workspace are displayed in tabs by default. If you are using the Reflection Ribbon, you can choose to display them in windows that can be tiled or cascaded.
Status bar	Using a combination of text and icons, the enhanced status bar displays information about the selected tab, such as the name and connection status of terminal sessions, or the URL of Web sessions, the screen mode, and the current transfer mode.
Task panes	When you select Screen History or productivity features such as Scratch Pad, task panes are opened next to the document tabs. These panes can be moved or resized, and their content can be saved as separate files.
	NOTE: To reopen the file later, it must be saved in a trusted location.

The size and location of the workspace, along with all open terminal sessions, Web pages, and task panes, is referred to as the layout. You can save the settings of a layout to a file. When reopened, a layout file automatically opens the saved documents and repositions the workspace to the specified size and location.

NOTE: If you are using the Classic user interface mode, you can arrange multiple sessions on your desktop and save them in a layout.

Documents

A document is a file that specifies the settings and behavior of a terminal session, a Web page, a printer session, or an FTP client session.

When you open a document, the related session or Web page is opened, either in the workspace (for terminal sessions and Web pages) or in a separate window (for printer sessions and FTP client sessions).

The document for a terminal session contains configuration settings for host-specific information. It also includes pointers to other files that are used to control the appearance of the session, such as the theme file, and to files that control input and text handling, such as the keyboard map file and the Ribbon file.

You can open any number of terminal sessions or Web pages in the workspace.The document name appears on the tab label unless a different name has been specified in a layout. The name of the selected document appears in the title bar of the workspace.

Appearance

You can control the appearance of documents in the workspace using themes, which combine color specifications for text and backgrounds, cursor types, and sounds for session-level events.

You can also select a color scheme for the workspace and ribbon background and sounds for workspace events.

In this Chapter

- "Manage Themes Dialog Box (6530 Sessions)" on page 237
- "QuickPads" on page 239
- "Workspace Settings Dialog Box" on page 241
- "CommandCast Panel" on page 242

Configuring Reflection

There are two types of configuration available in the Reflection workspace: *session document* and *workspace* configuration.

The document for a terminal session contains configuration settings for host-specific information. It also includes pointers to other files that are used to control the appearance of the session, such as the theme file, and to files that control input and text handling, such as the keyboard map file and the Ribbon file.

NOTE

- There are no document configuration settings for Web page documents.
- Printer sessions and FTP client sessions open in windows outside the Reflection workspace. They are configured from within those windows, instead of the workspace.

Workspace configuration settings affect all terminal session and Web page documents opened in Reflection. Workspace configuration settings include security, file locations, and other settings related to Reflection.

If any settings are unavailable, they may have been disabled by your administrator. If this is the case, the User Account Control icon appears in the upper left corner of the workspace.

Clicking the **Change Currently Disabled Settings** link next to this icon allows an administrator to enable settings.

When you navigate to multiple settings pages, all the settings on all the pages are saved when you click **OK**, or discarded when you click **Cancel**.

Video

How To Use the Reflection Desktop Settings Window (2:44)

Related Topics

- Chapter 5, "Terminal Sessions," on page 245
- "Session Documents and Related Files" on page 246
- "Open a Web Session" on page 23

Using Layouts

In Reflection, the size, location, and arrangement of the workspace and any open terminal or Web session documents can be saved to a layout file. When opened, a layout automatically opens and arranges all documents saved to the layout, opens and positions any docked panes (such as Scratch Pad or Screen History), and connects session documents to configured hosts.

If the workspace is configured to display documents as tabs, you can create a name for each tab. This can be useful when you use two different applications on one host. You can create a session document that connects to that host, then open the document twice, add a different name to each tab, and then save your layout.

If you are using the Classic user interface mode, you can arrange multiple sessions on your desktop and save them in a layout. The next time you open the layout, you'll find everything in place just the way you left it.

In addition, by using layout files, you can access the Reflection .NET API in multiple instances of Reflection simultaneously.

NOTE: If you already have terminal session or Web session documents open when you open a layout, the layout opens in a new workspace.

Video

▶️ Creating and Using Layouts(1:52)

In this Section

Layout Settings Dialog Box

Getting there

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **File** menu or the Reflection button ⬦ (if using the Office 2007 Look and Feel), choose **Settings**, and then **Layout Settings**.
Reflection Browser	On the **Reflection** menu, choose **Settings** and then **Layout Settings**.
TouchUx	Tap the Gear icon and then select **Layout Settings**.
Classic or Classic MDI VT	From the Setup menu, choose **Layout Settings.**
Classic or Classic MDI IBM	From the Options menu, choose **Layout Settings**.

By using layout files, you can access the Reflection .NET API in multiple instances of Reflection simultaneously. From this dialog box, define how to access the API in the instance of Reflection that starts when you open a layout file. (You must also enable the API in the **Set Up API and Macro Security** dialog box.)

NOTE: Reflection doesn't prompt you to save changes to a layout.

Set Up API

Automation server name	Specify the name you'll use to access a particular Reflection instance. For example, you can specify this server name in VBA macros that use automation to get a running Reflection instance.
IPC channel name	Specify a channel name. This setting overrides the IPC channel name specified in the **Set Up API and Macro Security** dialog box for the saved layout. In your custom application, use this name to access the API in the Reflection instance that starts when you open the layout file. (**Use IPC** must be selected in the **Set Up API and Macro Security** dialog box.)

Video

▶ Creating and Using Layouts(1:52)

Related Topics

- "Set Up API and Macro Security Dialog Box" on page 434
- "Using Layouts" on page 141
- "Create or Modify a Layout" on page 40

Tab Properties Dialog Box

Getting there

1 Open a session document.

2 In the workspace, right-click the session document tab and choose **Tab Properties**.

Use this dialog box to add labels to tabbed documents saved with layouts. These labels appear on the tab in place of the actual filename when the document is viewed as part of a layout. This dialog box also provides a unique identifier for a document tab that you can reference in macros and scripts.

The location of the document tabs (top, bottom, left, or right) is selected on the **Configure User Interface** dialog box.

NOTE: Tab properties are lost if you close the associated document without saving a layout. These properties are used on the document tab only in the saved layout.

Name	Type a label to appear on the document tab in a saved layout. This text does not affect the filename of the document or the appearance of the tab when opening the document outside the layout.
Description	Type information relevant to the document or its use in the layout.
API tab identifier	Shows an alphanumeric identifier for the current instance of the tab. This number changes each time the document (tab) is opened. This read-only ID can be used to reference the tab through the API.
Document filename	Shows the full name, including the path, of the saved document file. The name of the document also appears in the title bar of the workspace. This value cannot be edited.

Related Topics

- "Create or Modify a Layout" on page 40
- "Configure Workspace Defaults Dialog Box" on page 221
- "Set Tab Colors" on page 42

Search

Reflection features a **Search** box at the upper right corner of the workspace, in the Help viewer, and in some settings dialog boxes.

Using the Search Box on the Workspace

The Search box on the workspace works differently for each Reflection interface mode.

Using Search with the Classic or Classic MDI interface mode

When using the Classic modes, the search only applies to the active document.

For IBM terminals, the search term is highlighted as shown.
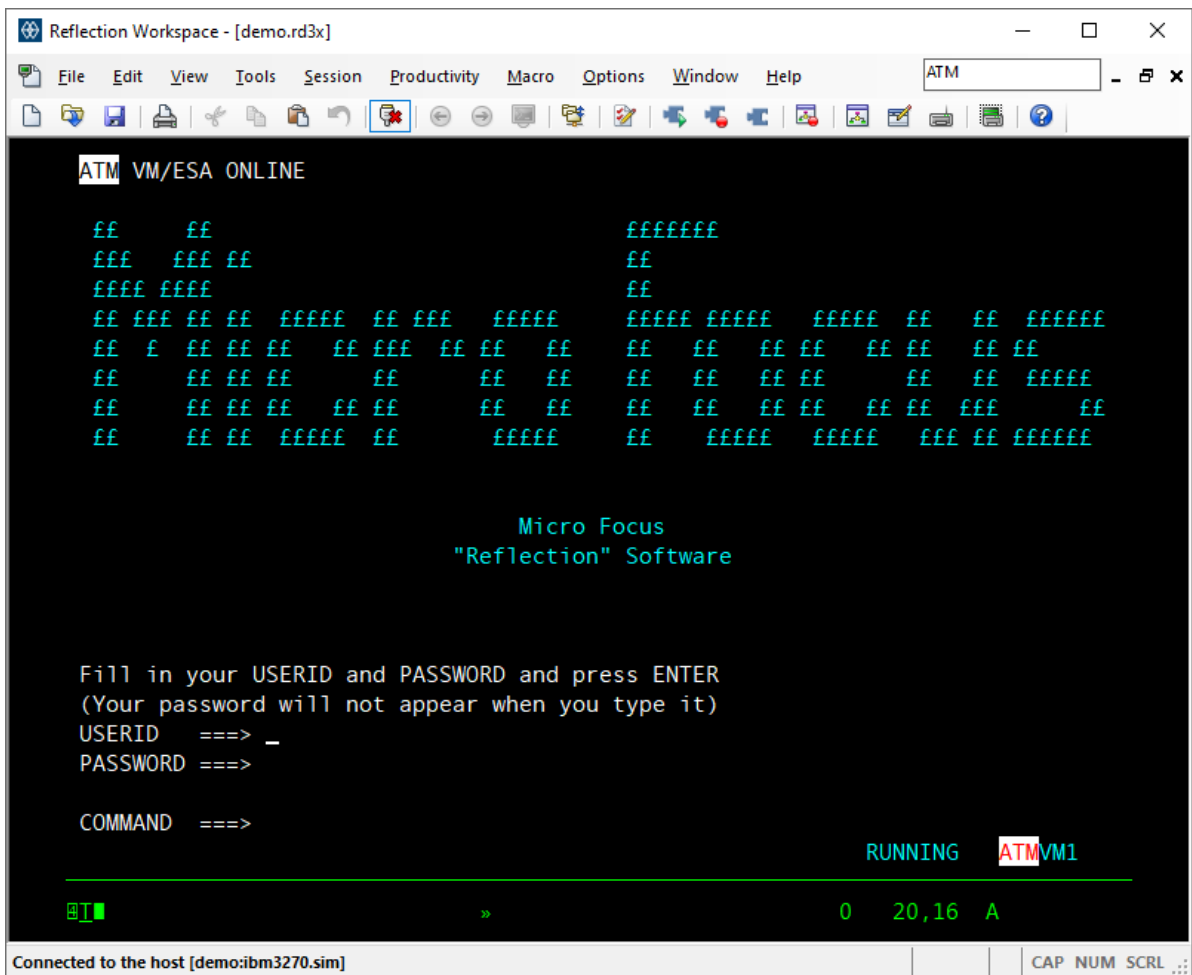
When using VT terminals in Classic mode, the search items are displayed in the Search Results list at the bottom of the workspace. You can click on these list items to go to the places in the session where the search term was found.

```
demo.rdox - Micro Focus Reflection Desktop                                    junk

 File   Edit   Connection   Setup   Macro   Productivity   Help

Technical Data and Computer Software clause in DFARS 252.227-7013.


                        Hewlett-Packard Company
                        3000 Hanover Street
                        Palo Alto, CA 94304 U.S.A.

Rights for non-DOD U.S. Government Departments and Agencies are as set
forth in FAR 52.227-19(c)(1,2).
demo: ls
OAIDERROR.console      inform              system
Mail                   jo                  test
News                   junk1               testfs
SYSBCKUP1              libs                testfs1
UPDATE_CDROM1          locate              testfs2
anyone                 lost                tmp
bin                    mail                usersa
dead.letter            map                 usersb
dump                   news                usersc
elder                  sam.pro             usr
etc                    space.profile       wrqdemo
harvest                spec
hp-ux                  swat
demo:

45,7 || Connected to the host [UNIX] (VT500-7)              CAP  NUM  SCRL  Hold
```

Using Search with the Ribbon interface

When using the Ribbon interface, you can use the Search box to perform a search of the open documents and screen history in Reflection, and for content on your desktop and on the Web.
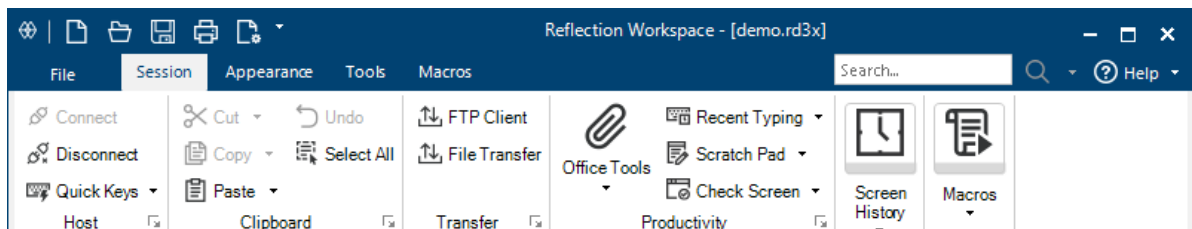
The following commands are available from the workspace Search menu:

Current Document Search	Searches only the selected document. Text matches are highlighted in the session (on-screen).

All Documents Search	Searches all open session or Web page documents.
	Search results appear in a separate pane at the bottom of the workspace. Double-click an item to highlight it in the session (on-screen).
Screen History Search	Searches the screen history of open terminal session documents.
	Search results appear in a separate pane at the bottom of the workspace. Double-click an item to highlight it in the session (on-screen).
Windows Desktop Search	Searches files and folders — including the content of text files and Microsoft Office files — on the desktop, using the Windows Desktop engine.
	Search results appear in a separate pane at the bottom of the workspace. Double-click a file to open it in the associated application.
Google Web Search	Searches the Internet using the Google search engine. Results appear in a new tab (Web page document) in the workspace.
Bing Web Search	Searches the Internet using the Microsoft Windows Bing search engine. Results appear in a new tab (Web page document) in the workspace.

Help

You can search the product Help from the **Search** tab in the Help navigation pane.

Settings Dialog Boxes

You can use the **Search** box from a dialog box to look for a word or part of a word in the various Reflection settings dialog boxes. At the top of the dialog box, search results that match your text, together with a navigation path, are displayed in a separate pane. Double-click an item to navigate to and highlight it in the identified settings dialog box.

This search finds only terminal session settings that are included in primary dialog boxes (those that have a **Search** box in the upper right-hand corner). It does not search settings in secondary dialog boxes (which include those dialog boxes associated with printer sessions, FTP client sessions, or file transfer). If you cannot find the setting for which you are looking with the settings search, use the index, or search the Help. The Help topic for the dialog box includes instructions for finding it in the product.

In some instances, the dialog box search may find settings that are functionally equivalent to the term you typed in the **Search** box. For example, if you enter `DBCS` in the **Search** box, the results will include the check box for **Support double-byte character set**.

Customize Ribbons, Menu, and Toolbars

You can customize the Ribbon or the Classic MDI menus and toolbars to suit your work needs. You can use the **UI Designer** to determine which controls to include and what they do, from simple tasks to complex routines. In addition to creating new controls, you can modify existing controls, remove controls you don't use, or relocate controls. Because the interface can be modified so that it is appropriate for the current terminal type, these changes are specific to each session type.

The Classic UI Designer

Getting there

1 Open a session document in the Classic user interface mode.

2 Open the Classic UI Designer:

   - For a VT session, on the **Setup** menu, choose **Toolbar**.

   - For other types of sessions, Choose **Settings** on the Options menu and then under **User Interface**, choose Manage **Ribbon**. Then choose **Modify the currently selected Ribbon file** or **Create a new Ribbon from an existing Ribbon file**. (When you are using the Classic MDI user interface mode, these Ribbon settings are actually toolbar and menu settings.)

With the UI Designer, you can create or modify the menus and toolbars that you use for the Classic interface mode. You can set up sessions to share the same customized menus and toolbars or you can set up unique menus and toolbars for each session.

After you customize menus and toolbars for a session and save these settings, you can apply them to other sessions. You can also import toolbars from Reflection 14 or Extra! sessions and then save them in Reflection `.xuml` files that can be applied to other sessions.

NOTE: For IBM sessions, only Extra! and Reflection Desktop toolbar files can be imported. For VT sessions, Extra!, Reflection Desktop, and Reflection 14 toolbar files can be imported.

The Design View displays a dynamic, graphical view of the menu and toolbars that you are creating or modifying. After you insert the controls, you can assign them to any of the actions supported by Reflection Desktop.

You'll save your changes in a custom UI file (.xuml) that you can use with other session documents.

NOTE: If the currently selected Custom UI file is one of the built-in files that is included in the installation folder, Reflection automatically creates an editable copy of the built-in file and saves the copy with your modifications to the `CustomUI` folder in your Reflection user data folder.

For more information, see:

"Customize Classic Menus and Toolbars" on page 109

"To import toolbars" on page 111

Video

▶️ How To Customize Menus and Toolbars in Reflection Desktop Classic Mode (3:40)

About the Ribbon

In the area between the Quick Access Toolbar and the document window is the Ribbon, a dynamic, collapsible device that organizes commands, buttons, and other controls on tabs for each task area.

Whether you're a system administrator or user, you can customize the Ribbon interface to make Reflection more convenient to use. For example, since the **Privacy Filters** button affects the way data is handled by the productivity features, you could add it to the **Productivity** group on the **Session** tab.

Using the **UI Designer**, you determine which controls to include and what they do, from simple tasks to complex routines. In addition to creating new controls, you can modify existing controls, remove controls you don't use, or relocate controls to other tabs.

You can also use the Reflection VBA or .NET API to dynamically show or hide custom Ribbon controls, enable or disable the controls, and change the actions that are mapped to the controls. (See Dynamically Changing the User Interface in the VBA Guide or the .NET API Guide.)

Manage Ribbon Dialog Box

Getting there

1 With a session open in Reflection, from the **Quick Access Toolbar**, click 📄.

2 Under **User Interface**, click **Manage Ribbon**.

The Ribbon contains tools that you use to complete tasks in the selected document. When you create a terminal session document, it includes a pointer to a default, built-in Ribbon file. For example, a new 5250 session document uses Reflection2007.5250.Ribbon.xuml (or Reflection2007.5250.Classic.xuml if you work in Classic mode). You can choose a different Ribbon file for each session, and you can create custom Ribbon files using the **UI Designer**.

Select another Ribbon file	Click to choose a different Ribbon file from a list of existing Ribbon files. The file must be in a trusted location.
Modify the currently selected Ribbon file	Select to open the UI Designer and modify the Ribbon file used by this session. Because built-in files are read-only, if the currently selected file is a built-in file, it will be saved as a custom file when you change it.

NOTE: If you select a Ribbon that doesn't match the current document type or user interface, the default Ribbon is used instead to ensure access to all features.

Create a new Ribbon from an existing file	Click to create a custom Ribbon file based on an existing Ribbon file. To reopen the file later, it must be saved in a trusted location.

Video

▶ Customizing the Ribbon (2:51)

Related Topics

 ◆ "Customize Ribbons, Menu, and Toolbars" on page 147
 ◆ "UI Designer" on page 149

Select a Ribbon File Dialog Box

Getting there

1 With a session open in Reflection, from the **Quick Access Toolbar**, click .
2 Under **User Interface**, click **Manage Ribbon**.
3 Click **Select another Ribbon file**.

From this dialog box, select a Ribbon file to use with this session.

Built-In	Select this option to show the Ribbon files distributed with Reflection.
Custom	Select this option to show the Ribbon files that you've previously modified and saved. If the file you want doesn't appear in the list, click **Browse** to select it.
	NOTE: The file must be in a trusted location.

UI Designer

Getting there

1 Open a session document.
2 On the **Appearance** tab, in the **Menus** group, click **UI Designer**.

With the UI Designer, you can create new controls — including buttons, tabs, and menus — or modify existing controls on the Ribbon. Save your changes as a custom UI file (`.xuml`) that you can use with other session documents.

Design View

Displays a dynamic, graphical view of the Ribbon and tabs. Navigate to and select the controls you want to modify.

Insert Controls

Click the items you want to add to the Ribbon.

Tab	Adds a Ribbon tab on which you can place additional controls.
Group	Adds a container for controls.
Button	Adds a single button control.
Gallery	Adds a menu of buttons.
Split Button	Adds a button and a menu.
Button Group	Adds a button that contains three individual button controls, including split buttons and button menus (Galleries).
Built-ins	Adds a control for built-in features, such as Quick Keys and Office Tools.

New items appear on the far right end of the Ribbon. If a button or group is selected in the Design View, new buttons appear in the same group as the selection.

Arrange Controls

Move Up Move Down Move Left Move Right	Moves the selected control in the direction specified.
Delete	Removes the selected control from the Ribbon.
Select Parent	Selects the parent control, or container, for the selected child or group control. NOTE: To select a button group, click the bottom edge of the group, or, select one of its buttons, and then, under Arrange Controls, click Select Parent.

Review

Preview	Displays, in a separate window, the way the Ribbon will appear with the options you selected.

Settings

This area of the UI Designer displays, for the selected control, the settings that allow or require additional input.

The specific items shown will vary, depending on the control that is selected.

Show dialog launcher button	Select to add a dialog launcher button next to the label on a Group.

Identifier	Use to identify the control when programming with the Reflection API.
	NOTE: See "Dynamically Changing the User Interface" in the VBA Guide or the .NET API Guide.
Visible	Select to display the control. You can use the Reflection API to show or hide the control.
Enabled	Select to enable the control. You can use the Reflection API to enable or disable the control.
Action	Shows the action assigned to the control.
Select Action	Click to specify an action for the selected control in the **Select Action** dialog box.
Modify Subitems	Click to add subitems to a control. For example, if you add a gallery to a button group in the Subitems Collection Editor dialog box, click Modify Subitems to add buttons to the menu for that gallery.
Change settings	Select to allow changes to the label, image, tooltip, and description of the control.
	NOTE: Changes to these settings overwrite the default properties of the selected action.
Label	Specifies the text that appears on the control.
	If you select an action that is set up to be controlled with a toggle switch (for example, the Connect/Disconnect action), another set of label boxes and images are displayed so you can set the default and selected labels along with their associated images.
	NOTE: An ampersand (&) in front of a character in a label indicates that the character will function as a keyboard accelerator key.
Image	Shows the image that appears on the control.
	Click **Select** to browse for a .PNG or .JPEG image to appear on the control.
	Click **Remove** to remove the image and display only the label for the control without an image.
Tooltip	Enter a heading that appears when the pointer is held over the control.
Description	Enter a description that appears (below the heading) when the pointer is held over the control.
Reset	Click to clear any of changes you've made and restore the default properties of the assigned action.

Video

▶ Customizing the Ribbon (2:51

Related Topics

- "Add Controls to the Ribbon" on page 101

Create a New Ribbon File Dialog Box

Getting there

1 With a session open in Reflection, from the Quick Access Toolbar, click ⬚.

2 Under **User Interface**, click **Manage Ribbon**.

3 Click **Create a new Ribbon from an existing Ribbon file**.

From this dialog box, select the Ribbon file to use as a template for creating a new Ribbon file.

Built-In	Select this option to show the Ribbon files distributed with Reflection.
Custom	Select this option to show the Ribbon files that you've previously modified and saved. If the file you want doesn't appear in the list, click **Browse** to select it. **NOTE:** The file must be in a trusted location.
Use the new file in the current session document	Select this option to use the file you are about to create with the current session.

Subitems Collection Editor Dialog Box (UI Designer)

Getting there

1 Open a session document.

2 On the Ribbon, click the **Appearance** tab.

3 From the **Menus** group, click **UI Designer**.

4 Under **Insert Controls**, click **Gallery**, **Split Button**, or **Button Group**.

-or-

Select an existing **Gallery**, **Split Button**, or **Button Group**, and then, under **Settings**, click the **Modify Subitems** button.

If you add a button group, split button, or gallery control to the Ribbon, you must specify subitems (buttons and menus) for that control.

Choose from the available subitems:

Subitems

Add	Add a **Button**, **Split Button**, or **Gallery** to a control. The control you select in the **Insert Controls** pane of the **UI Designer** determines the subitems you can add; for example, if you select **Button Group**, you can select any of the subitems.
Remove	Removes the selected control type from the list.
Move Up / Move Down	Moves the selected control up or down in the list.

Subitem Settings

Identifier	Use to identify the control when programming with the Reflection API.
	NOTE: See "Dynamically Changing the User Interface" in the VBA Guide or the .NET API Guide.
Visible	Select to display the control. You can use the Reflection API to show or hide the control.
Enabled	Select to enable the control. You can use the Reflection API to enable or disable the control.
Action	Shows the action assigned to the control.
Select Action	Click to specify an action for the selected control in the **Select Action** dialog box.
Modify Subitems	Click to add subitems to a control. For example, if you add a gallery to a button group in the Subitems Collection Editor dialog box, click Modify Subitems to add buttons to the menu for that gallery.
Change settings	Select to allow changes to the label, image, tooltip, and description of the control.
	NOTE: Changes to these settings overwrite the default properties of the selected action.
Label	Specifies the text that appears on the control.
	NOTE: An ampersand (&) in front of a character in a label indicates that the character will function as a keyboard accelerator key.
Image	Shows the image that appears on the control. If you don't select an image, an orange circle with an exclamation point appears.
Select Image	Click to browse for a .PNG or .JPEG image to appear on the control.
Tooltip	Enter a heading that appears when the pointer is held over the control.
Description	Enter a description that appears (below the heading) when the pointer is held over the control.
Reset	Click to clear any of changes you've made and restore the default properties of the assigned action.

Related Topics

- "Select Action Dialog Box" on page 253
- "Add Controls to the Ribbon" on page 101

Built-In Controls Dialog Box (UI Designer)

Getting there

1 Open a session document.

2 On the **Appearance** tab, in the **Menus** group, click **UI Designer**.

Reflection includes several controls that you can customize. With **UI Designer**, you can change the default location and settings of these controls to better suit your needs.

Click **Built-Ins** in the **Insert Controls** pane of **UI Designer** to choose from the following options:

Quick Keys Gallery	Add keyboard shortcuts that let you send program function keys, program attention keys, and other commands to the host.
Office Tools Gallery	Use Microsoft Word and Outlook application features with data from your host: create Word documents, send e-mail, schedule appointments, add notes and tasks, and create new contacts.
Recent Typing Gallery	Quickly view and select from a list of recently typed items, and send the selected string to the active document, eliminating the need to re-enter information. This saves time and reduces errors when entering commonly-typed commands or field data.
Scratch Pad Gallery	Keep notes associated with a session using the Scratch Pad, and print or save them as .rtf or .txt files.
Screen History Gallery	View and/or verify the information from Screen History recordings of host screens as you navigate them, and send multiple host screens to Microsoft Word, PowerPoint, and Outlook (Email Message and Note only), if they're installed on your computer.
Colorpicker Control	Add a control for standard and custom colors for host sessions.
VBA / Macro Group	Provide the Visual Basic editor, and macro recording and playback tools.
Themes Group	Set the appearance of host sessions, including text and background colors, sounds, and cursor properties.

Locking Down the User Interface

Getting there

- From the Reflection installation folder, run `AccessConfig.exe`.

Use Permissions Manager to restrict access to Reflection features. After you select the features you want to disable, your specifications are saved in `.access` files that you can deploy to users.

NOTE: You can restrict access to Reflection controls only on systems on which the Windows User Access Control (UAC) is enabled. If the UAC is disabled, the configuration settings that restrict access do not apply.

Permissions Manager displays groups of configurable items.The following reference topics provide a brief description for each item.

Actions Group (page 157)

3270 Terminal Groups

Clipboard (page 178)

Connection\TN3270 Advanced (page 164)

Connection\TN3270 Basic (page 166)

Terminal\Configuration\3270 (page 167)

5250 terminal Groups

Clipboard (page 178)

Connection\TN5250 Advanced (page 171)

Connection\TN5250 Basic (page 173)

Terminal\Configuration\5250 (page 174)

VT terminal Groups

Clipboard (page 191)

Connection (page 191)

Safeguards (page 195)

Terminal (page 193)

Workspace Groups (page 185)

Api Security (page 185)

Application Options (page 185)

Application Sounds (page 187)

PCI DSS (page 188)

Privacy Filter (page 189)

Trusted Locations (page 189)

UX Configuration (page 189)

Document Groups

Classic (page 181)

Hotspots (page 180)

Keyboard (page 181)

Mouse (page 181)

Ribbon (page 181)

Theme (page 182)

6530 terminal Groups

Productivity Groups

Clipboard

Connection\Security

Connection\Security\SSH

Connection\Security\SSL

Connection\TN6530\Advanced

Connection\TN6530Basic

Input Devices\AID

Productivity\RecentTyping

Terminal\Configuration\6530

Terminal\Configuration\DisplaySettings

Theme

Productivity (page 183)

AutoComplete (page 184)

AutoExpand (page 184)

Office (page 184)

RecentTyping (page 183)

ScreenHistory (page 183)

SpellCheck (page 182)

Security Groups

Security\PKI

Security\TLS

Related Topics

◆

How the Permissions Manager Items are Organized

Groups   The feature group to configure.

Items   Lists the configurable items within the selected group.

This column	Indicates
Item	The name of the item.
Accessibility	The security level of the item. **Full** means that the user can configure the item; **Restricted** means that the user cannot configure the item without administrator assistance.

Permissions Manager Additional security options

Session File Encryption

Session files may be encrypted from the **Save As** dialog box, by selecting the encrypted option from the **Save As Type** box.

User Can Only Open Encrypted Session Files	Select to prevent the user from opening unencrypted session files.
User Can Only Save Encrypted Session Files	Select to prevent the user from saving unencrypted session files.
User can create session update files	Select to allow users to save session update files.

Restrict Actions (actions.access)

In many cases, an action can be accessed multiple ways. For example, you can restrict access to the Clipboard Settings action (clipboardSettingsAction). However, if the user has access to the Document Settings action (settingsAction), Clipboard settings will still be accessible.

Item Name	UI Description
abortFileTransferAction	Does not apply to Reflection.
appointmentAction	Create an Outlook appointment that includes the selected host data in the message field.
backHistoryAction	View the previous host screen in ready-only mode.
captureIncomingDataAction	Capture data received from the host and save it to a file.
checkForUpdateAction	Open the Reflection solution library on the Micro Focus support Web site and access the latest product downloads.
clearAllAction	Remove all text from the display memory, including what's on the screen.
clearDisplayAction	Remove all text from the screen. By default, Reflection saves this text to the display memory.
clearScreenAction	Remove all text from the screen. By default, this text is saved to the display memory.
clearSelectionAction	Clear the selection by clicking somewhere.
clipboardSettingsAction	Open the **Clipboard Settings** dialog box to configure settings that control how the Cut, Copy, and Paste functions work.
closeAction	Close the current document.
codePageSettingsAction	Open the **Select Host Code Page** dialog box to specify the host code page for your display session.
connectAction	Connect to the host for the current session document.
connectDisconnectAction	Connect to the host for the current session document, and then invoke again to disconnect.
contactAction	Create a new contact in Outlook that includes the selected host data in the Notes field.
contextMenuEditorAction	Open the Context Menu Editor.
copyAction	Copy the selected text to the Clipboard.
copyAppendAction	Add the selected text to the Clipboard.
copyTableAction	Copy data in a tabular format.
CopyToBuffer1Action	Does not apply to Reflection.
CopyToBuffer2Action	Does not apply to Reflection.
CopyToBuffer3Action	Does not apply to Reflection.

Item Name	UI Description
CopyToBuffer4Action	Does not apply to Reflection.
createPlusFromHistory	Export screens to be used in the Screen Designer.
createSplitScreenAction	Does not apply to Reflection.
cutAction	Delete the selected text and copy it to the Clipboard.
cutAppendAction	Delete the selected text and add it to the Clipboard.
cycleDocumentsAction	Makes a session document or a Web page active on an MDI workspace whether you are viewing your documents as tabs or windows or make a workspace active if SDI mode is used.
disconnectAction	Disconnect from the host for the current session document.
displayAttributesAction	Does not apply to Reflection.
documentPropertiesAction	Shows the properties associated with the current tab. Tab properties are associated with layout files, not with the session document.
editCaslMacroAction	Does not apply to Reflection.
emailMessageAction	Create an Outlook e-mail message that includes the selected host data.
eventUIMapperAction	Map predefined event to one or more actions.
exportRPlusHistoryAction	Export the current screens to be used in the Plus Designer.
fileTransferAction	Open the **Transfer** dialog box.
forwardHistoryAction	View the next screen in your screen history sequence.
ftpFileTransferAction	Open Reflection FTP Client.
fullScreenViewAction	Hide the Ribbon, and expand the workspace to fill your computer screen.
globalSettingsAction	Open the Reflection workspace configuration settings. Workspace configuration settings affect all terminal session and Web page documents opened in Reflection. Workspace configuration settings include security, file locations, and other settings related to Reflection.
helpAction	Open Help from the main workspace **Help** button.
hostConnectionSettingsAction	Configure the host connection for the current session document.
hotspotsSettingsAction	Open the **Set Up Hotspot Display Settings** dialog box.
keyboardExtendSelection	Extend the screen selection using the keyboard.
keyboardMapperAction	Display the keyboard map.
launchApplicationAction	Launch an external application from the Reflection workspace using a customized UI element.

Item Name	UI Description
launchRPlusDesignerAction	Launch Screen Designer to customize the appearance of Host Screens.
launchSupportWebsiteAction	Open the Micro Focus Support site from the **Help** menu.
launchVbaAction	Open the Visual Basic editor to create a VBA macro based on objects defined by the active session.
layoutCascadeAction	Arrange all open document windows in a cascade. The title bar of each window remains visible.
layoutHorizontalAction	Arrange all open document windows horizontally.
layoutSettingsAction	Open the **Layout Settings** dialog box.
layoutVerticalAction	Arrange all open document windows vertically.
lightPenAction	Simulate a light pen selection with your mouse or keyboard.
macroSecurityAction	Set macro security options to protect a macro from accidental changes.
mainframeTransferChunkAction	Open the **Transfer Settings** dialog box.
manageRibbonSettings	Configure the selected ribbon or classic UI mode file. You can select another ribbon file, modify the current file, or create a new file.
manualCaptureAction	Manually capture the current screen.
mapKeystrokeAction	Open the **Keyboard Mapper** to associate a keystroke with a host terminal key or to create a keyboard shortcut.
modelSettingsAction	Open the basic host connection settings page to specify the terminal model you want to emulate.
modifyThemeAction	Open the Modify Theme dialog box to change settings such as font, text color, or background color.
moveCursorAction	Move the cursor with a mouse click.
moveHostCursorAction	Move the cursor by sending the correct arrow keys to the host so that it moves the cursor relative to its current position.
newDocumentAction	Create a new document of any kind from the "Reflection Workspace menu" on page 897 or the **Quick Access** toolbar.
nextDocumentAction	Make the next document active on an MDI workspace or make the next workspace active if SDI mode is used.
nextWindowAction	Make the next document or task pane active.
noteAction	Create an Outlook "sticky" note that includes the selected host data.
officeToolsPaneAction	Open the **Office Tools** task pane.
openAction	Open any kind of document from the "Reflection Workspace menu" on page 897 or the **Quick Access Toolbar**.
openDocumentAction	Open existing session documents, layout files, or Web pages.

Item Name	UI Description
openEmlEditorAction	Open the Express Macro Language (EML) editor.
openURLAction	Open a Web page from within Reflection.
pageSetupAction	Open the Page Setup dialog box.
pasteAction	Paste data from the Clipboard to the current cursor location.
PastefromBuffer1Action	Does not apply to Reflection.
PastefromBuffer2Action	Does not apply to Reflection.
PastefromBuffer3Action	Does not apply to Reflection.
PastefromBuffer4Action	Does not apply to Reflection.
pasteNextAction	Insert the remaining text in the paste next buffer within the host application.
pasteRangeAction	Open the Paste Range dialog box to paste data into a screen region.
pathDBEditorAction	Does not apply to Reflection.
pathWizardAction	Does not apply to Reflection.
pauseCaptureAction	Pause the Macro recording process.
pauseMacroAction	Pause a recording macro.
playBackTraceAction	Select a trace file to play back.
playNextTraceRecordAction	Play the next record in the current trace file.
playPreviousTraceRecordAction	Play the previous record in the current trace file.
previousDocumentAction	Make the previous document active on an MDI workspace or make the previous workspace active if SDI mode is used.
printAction	Print the current document from the "Reflection Workspace menu" on page 897 or the Quick Access toolbar.
printAllSplitScreens	Does not apply to Reflection.
printMultipleScreensAction	Open the Print Multiple Screens pane to capture screens and then print them.
printSetupAction	Open the Print Setup dialog box.
processRUOTraceAction	Process a trace file to generate a Reflection Basic script file, or to add system details to the text format report.
productivityFieldSecurityAction	Switch Field security on or off. When Field Security is on for a field, Screen History, Office Tools, and all of the productivity features are disabled for that field.
ptrRouteWizardAction	Does not apply to Reflection.
ptrStatusPanelAction	Does not apply to Reflection.
quickKeysAction	Open a gallery of buttons that you can click to send PA keys, PF keys, or other commands to the host.

Item Name	UI Description
quickPadSettingsAction	Open the Manage QuickPads dialog box from which you can create, modify, and select quickpads.
quickPrintAction	Print the current document without opening the Print dialog box.
receiveFileTransferAction	Does not apply to Reflection.
recentTypingPaneAction	Open the Recent Typing task pane.
recordExpressMacroAction	Record an Express macro.
recordMacroAction	Record a VBA macro.
resetConnectionAction	Does not apply to Reflection.
resetTerminalAction	Does not apply to Reflection.
runCaslMacoAction	Does not apply to Reflection.
runEBEditAction	Run Extra! Basic Editor.
runExpressMacroAction	Run an Express macro.
runHostExplorerMacro	Run a macro that contains Hummingbird Basic commands.
runLegacyExtraMacroAction	Open an Extra! file that contains macros, and select one to run.
runLegacyMacroAction	Run an embedded legacy Reflection macro.
runLegacyMacroWithDataAction	Run an embedded legacy Reflection macro with data. (This allows the user to type parameters to execute with the macro.)
runLegacyRBEditAction	Run Reflection Basic Editor.
runLegacyRBMacroAction	Run a legacy Reflection Basic macro.
runLegacyReflectionMacroAction	Run an external legacy Reflection macro.
runMacroAction	Run a Reflection Workspace macro.
runPcommMacroAction	Open an IBM Personal Communications file that contains a macro.
RunQWSMacroAction	Open a QWS3270 file that contains a macro.
runRCLScriptAction	Run an RCL script.
runRumbaMacroAction	Open a Rumba file that contains macros, and select one to run.
runSupportToolAction	Runs a utility to help Micro Focus Support collect Reflection application data
saveAction	Save the current document from the "Reflection Workspace menu" on page 897 or the Quick Access Toolbar.
saveAsAction	Save the current document with a new name or location.
saveLayoutAction	Save the current layout.
saveRSFTAction	Save the current document configuration as a template.
scratchPadPaneAction	Open the Scratch Pad task pane.

Item Name	UI Description
screenHistoryPaneAction	Open the **Screen History** task pane.
selectAllAction	Select all data on the screen.
selectNextSplitScreenAction	Does not apply to Reflection.
selectNextSplitSessionAction	Does not apply to Reflection.
selectPreviousSplitScreenAction	Does not apply to Reflection.
selectPreviousSplitSessionAction	Does not apply to Reflection.
selectRPlusProfileAction	Select the Plus Customization File to be used with this session.
sendAPLKeyAction	Send a preconfigured APL key to the host.
sendFileTransferAction	Does not apply to Reflection.
sendHostKeyAction	Send a preconfigured key to the host.
sendHostTextAction	Send some preconfigured text to the host.
sendWordAction	Send the word at the current cursor location to the host, followed by a Return (VT) or an Enter (3270/5250) key. This is typically mapped to a mouse button.
setHotspotFileAction	Set the hotspots file for a session.
setKeyboardMapAction	Set the keyboard map file for a session.
setRibbonFileAction	Set the Ribbon file for a session.
setThemesFileAction	Set the theme file for a session.
settingsAction	Open the document settings from the "Reflection Workspace menu" on page 897 or the Quick Access Toolbar.
setupLoggingAction	Open the **Logging Settings** dialog box.
showAPIGuideAction	Open the .NET API Guide.
showAPIHelpAction	Open the .NET API Help.
showAutoCompleteSettingsAction	Open the **Configure Auto Complete** dialog box.
showAutoExpandAction	Open the **Configure Auto Expand** dialog box.
showContextMenuAction	Open the context menu. This is the default action of the right mouse button.
showHelpAboutAction	Show the **About** dialog from the **Help** menu.
showICPathSettingsAction	Does not apply to Reflection.
showLiveScreenAction	Return to the current host screen for your session from anywhere in the screen history sequence.
showMacroPanelAction	Show or hide the Macro Panel.
showMouseMapperAction	Open the **Mouse Mapper**.
showPrivacyFilterAction	Open the **Set Up Privacy Filters** dialog box.

Item Name	UI Description
showProductivitySettingsAction	Open the **Configure Productivity Defaults** dialog box.
showQuickPadAction	Show QuickPads mapped to the action or select which QuickPads to display.
showRecentTypingSettingsAction	Open the **Configure Recent Typing** dialog box.
showScreenHistorySettingAction	Open the **Configure Screen History** dialog box.
showSpecificContextMenuAction	Specifies the context menu to open when the action is performed.
showSpellCheckAction	Open the **Configure Spell Checking** dialog box.
showTabbedViewLayoutAction	Enables the "Arrange documents as tabs" setting.
showToolbarAction	Show toolbars mapped to the action or select which toolbars to display.
showUIDesignerAction	Open the UI Designer to customize your Ribbon.
showVBAGuideAction	Open the VBA Guide.
showVBAHelpAction	Open the VBA Help.
spellCheckFieldAction	Check spelling in the currently active host field.
spellCheckScreenAction	Check spelling in the current host screen.
sshConnectionSettingsAction	Open the Secure Shell Settings dialog box to configure Secure Shell connection.
startCaptureAction	Does not apply to Reflection.
startLoggingAction	Turn logging on for a VT session.
startTraceAction	Create a new trace and begin the trace process.
stopCaslMacro	Does not apply to Reflection.
stopLoggingAction	Turn logging off for a VT session.
stopMacroAction	Stop the currently running macro.
stopTraceAction	Stop the currently active trace.
taskAction	Create an unscheduled Outlook task that includes the selected host data in the task body field.
telnetAction	Launch Windows Telnet client.
terminalAppearanceSettingsAction	Open the **Configure Terminal Settings** dialog box.
themeSettingsAction	Open the **Manage Themes** dialog box.
toggleAPLModeAction	Turn APL mode on or off.
toggleAutoCompleteSettingsAction	Toggle Auto Complete settings including presentation of suggestions and handling of field data.
toggleClassicMenuBarAction	Show or hide the Classic menu bar.
toggleClassicStatusBarAction	Show or hide the Classic status bar.

Item Name	UI Description
toggleSessionUpdateAction	Specify a document settings update file and choose whether to save changes after an update.
toggleLoggingAction	Starts or stops logging text from a host session to a printer or file.
toggleMacroRecordAction	Record your actions in a VBA macro.
togglePauseMacroAction	Pause the macro recording process.
toggleRibbonStateAction	Show or hide the Ribbon.
toggleRPlusAction	Enable or Disable Plus screen customizations.
toggleStatusBarAction	Show or hide the status bar.
toggleTerminalKeyboardAction	Show or hide the-on screen terminal keyboard for the current session.
traceCaslMacroAction	Does not apply to Reflection.
undoAction	Undo the last cut or paste.
vbaMacroDialogAction	Open the Run Macro dialog box to select a macro to run.
wordDocumentAction	Create a Word document that includes the selected host data.

3270 Items

In this Section

Permissions Manager Items: TN3270 Advanced

TN3270 Advanced

Item Name	Sub-group	UI Description
AssociatedPrinterSession		The associated 3270 printer session filename.
AssociatePrinterBy	TN3270 Enhanced Protocol	The associated 3270 printer session, or Association string.
AsyncTransportEnabled		Revert to polling mode for host interactions. This is mainly used for diagnostic purposes.
AttentionKey	TN3270-specific	Treat ATTN key as TelnetAbortOutput, TelnetBreak, or TelnetIntProcess.
AutoReconnect		Reconnect after a disconnection that is not initiated by Reflection.
BackSpaceKeyAsDelete		Treat Backspace key as Delete key.

Item Name	Sub-group	UI Description
BeforeConnectStartupMacro		Run a macro or other action before the initial connection.
ConnectMacro	**Connection Action**	Run a macro or other action after the initial connection.
ConnectMacroData		The name of a macro that is run automatically after a connection is established.
ConnectScript		The Reflection script that runs automatically after a connection is established.
ConnectScriptArguments		The parameter string to pass to the connect script after a connection is established.
DBCSUnmappedChar		Allow user to choose how to translate double-byte host characters that are not available in the Shift-JIS double-byte character translation table.
EnableAssociatedPrinter		Enable the associated printer. (See AssociatePrinterBy, AssociatedPrinterSession, and TNAssociation.)
ExpressLogonFeature AppID	**Security**	The application ID to use for Express Logon Feature (ELF) support.
FileSystem		Allow users to specify whether to use the ANSI character set or the ASCII character set for ASCII transfers from the host.
HLLAPILongName	**HLLAPI Options**	The HLLAPI application associated with a particular session.
HLLAPIShortName	**HLLAPI Options**	An identifier that a HLLAPI application uses to link to a session.
HLLAPIStyle	**HLLAPI Options**	The HLLAPI configuration. This can be a numeric value or a predefined constant.
KeepAlive	**Misc.**	Periodically poll the host to determine if Telnet connections remain active during intervals when you are not sending data to the host.
KeepAliveTimeout	**Misc.**	The interval, measured in seconds, between keep alive requests sent by Reflection.
ReuseMSSNAPoolName		Allow users to choose how to handle MS SNA pool names. When unselected (the default), administrators must assign the pool to each user for the number of connections the user needs. When selected, administrators can assign the pool once to each user.
RunMacroAtReconnect	**Connection Action**	Run macro when reconnecting.
SameModel	**TN3270-specific**	Specify to use the same model for primary and alternate screens.

Item Name	Sub-group	UI Description
SecurityDialog		Open the Security Properties dialog box to set up secure data communications with SOCKS or SSL/TLS.
Support3270Partitions		Send partition-related information from the terminal to the host in response to a host query request.
SysReqKey	TN3270-specific	Specifies what happens when you transmit the SysReq function. The definition of this key varies by host application.
TelnetLocation	Misc.	The location where the connection originated. This can also be used to provide informational messages to the host from the PC.
TelnetResponseMode	TN3270Advanced	Return a message to the host from the PC after each message sent by the host.
TNAssociation		A 3270 terminal session on the host. Use this to associate a 3270 terminal session with a specific 3270 printer session.
UserDataDirectory		The folder where user-created files, like settings files and trace files, are saved by default.

Related Topics

Permissions Manager Items: TN3270 Basic

TN3270 Basic

Item Name	Sub-group	UI Description
AutoConnect	Host Connection Options	Automatically connect to the host.
ConnectionTimeout		The time period (in seconds) that Reflection waits for a host connection response.
CustomColumns	Text Display	The number of columns in the terminal window display when configured to use the custom terminal model.
CustomRows	Text Display	The number of rows in the terminal window display when configured to use the custom terminal model.
DeviceName	Connection	The device to connect to.
EnableConnectionTimeout		Enable or disable connection timeout.
ExitOnDisconnect		Automatically close the session when a session is disconnected.

Item Name	Sub-group	UI Description
GraphicsDevice	Graphics Display	The type of graphics device to emulate for 3179-G terminal sessions.
GraphicsEnabled	Graphics Display	Enable graphics.
Host	Connection	Host name/IP address.
ModelID	Text Display	Model ID.
Port	Connection	Port.
PromptReconnect		Prompt to confirm whether to disconnect a session when a session is disconnected manually or by closing the session or the workspace.
TerminalType	Text Display	Terminal/Device type.
TN3270Extended	Host Connection Options	Use Telnet Extended.
UseIDManagement		Set up ID Management. To use ID Manager, you'll need access to a centralized management server with ID Manager configured.

Related Topics

Permissions Manager Items: 3270 Terminal Configuration

Item Name	Sub-group	UI Description
AllowInvalidThaiInput		Turn off validity checking for Thai characters. (By default, when you enter Thai characters in a host application, Reflection determines whether the input is legal according to the rules of Thai character composition.)
AutoIME		Automatically turn the Input Method Editor (IME) on when the cursor is in a double-byte input field, and off when the cursor is in a single-byte input field. When it is not specified, the state of the IME does not change in response to the cursor's location.
BDTIgnoreScrollLock		Ignore the state of Scroll Lock.
C370CharSet		Use the C/370 code page. The C/370 code page provides support for square brackets ("[" and "]").
Caption		Specifies the string that appears in the Reflection title bar when running in Classic mode. This string is also displayed on the taskbar when Reflection is running.

Item Name	Sub-group	UI Description
CmdPrompt		The character or characters in the terminal window, after which Reflection attempts to insert Quick Text.
CMSFileListCommand		The file list command to issue on the CMS host to list files. When the Show host files button in the Transfer dialog box is clicked, Reflection issues the specified file list command.
CommandLineEnabled		Enable the Reflection command line. This allows users to activate the command line (for example, with the Alt-L keystroke).
CountryExtended GraphicsCode		Enable country-specific extended code page.
CursorMovementStyle		Specifies how the cursor moves between composed Thai characters.
CursorProgressionIndicator		Specifies how Reflection responds when the host queries to determine if End User Interface (EUI) enhancements are supported by the terminal. Use only for host applications that use cursor progression and queries to determine if EUI is supported.
DelayAfterAID		The amount of time, measured in milliseconds, to wait before processing keystrokes after an AID key (PF1-PF24, Enter, or Clear) is pressed.
DisplayMargins		Display margins around the terminal window.
EnableHotspots	Display	Enable all defined hotspots
EnableQuickText		Use the Quick Text feature.
EnterKeyRepeat		Specifies whether holding down the Enter key is equivalent to pressing it multiple times.
ExtendHotSpots		Treat a region to the right of a hotspot as part of the hotspot.
GraphicsExtendedColors		Use the set of extended graphics colors (black, white, dark blue, orange, purple, dark green, dark turquoise, mustard, gray, and brown).
HostBeep		Enable host beep.
HostCodePage		Host Code page.
HostKeyboardType	Input	The keyboard type.
HostNumlockControl		Allows the host to turn NumLock on.
HotspotsAltKey	Activation	Under Choose key(s) to press in combination with mouse click, activate the Alt key.
HotspotsCtrlKey	Activation	Under Choose key(s) to press in combination with mouse click, activate the Ctrl key.

Item Name	Sub-group	UI Description
HotspotsDoubleClick	Activation	Under **Choose key(s) to press in combination with mouse click**, activate the double-click action.
HotspotsMouseButton	Activation	Choose the mouse button to activate hotspots.
HotspotsShiftKey	Activation	Under **Choose key(s) to press in combination with mouse click**, activate the Shift key.
IgnoreHostPrintreq		Ignore print commands in host data streams.
InputFieldUnderlines		Specify how Reflection underlines input fields on host screens.
InsertArena		Specify the extent to which the **InsertProtocol** property applies — to a single field, across multiple local fields, or to all unprotected fields.
InsertProtocol		Specify how a character will be inserted.
KanaLockState		Specify the current Kana mode of the keyboard. When the keyboard is in Kana mode, it is capable of producing half-width Katakana characters. When it is not in Kana mode, the keyboard is in Latin character mode.
KeyboardErrorReset	Input	Keyboard error.
KeysDuringWait		Allow the user to use the keyboard during a synchronous command. A synchronous command (such as **Wait** or **WaitEvent**) causes a procedure to pause until a defined waiting period expires.
MappedNumlockPreservesNumlock		Specify how Reflection behaves if a user presses the PC NumLock key when it has been mapped to emulate the action of a terminal key.
MouseShape		Specify the appearance of the mouse pointer in the terminal window.
NumberMouseButtons		Specify how many buttons Reflection assumes the mouse has. Changing this property changes the mouse shown in the **Mouse Setup** dialog box.
Preserve3270insertState		Specify whether pressing Enter resets the Insert mode.
PreserveEntryMode		Remain in Extended Graphics or Hexadecimal mode indefinitely after either mode is entered. From Extended Graphics mode users can enter multiple graphics; from Hexadecimal mode users can enter hexadecimal characters.

Item Name	Sub-group	UI Description
QuickText		Specify the contents of the Quick Text buffer.
RectangularSelection		Specify that dragging the mouse across an area selects only the text within that area. When this option is cleared (unchecked), the selection wraps to line ends.
RightControlKeyRepeat		Designates the right Ctrl key as a modifier key. (A modifier key is used in combination with another key to send a function. For example, Ctrl-F1 is mapped to the Attention key in 3270 sessions).
ShowBytesRemaining		Display the Show Bytes Remaining indicator on the host status line. This indicator displays the number of bytes remaining in the current field.
ShowDisplayCharsInUppercase		Display characters in uppercase.
ShowHotspots	Display	Show all defined HotSpots.
ShowMenuBar		Display the menu and toolbar in Classic mode.
ShowOIA		Show operation and status messages in the Operator Information Area (OIA) at the bottom of the terminal window.
ShowSOSIChars		Show shift-out and shift-in (SO/SI) control characters on the terminal screen. (This helps to determine where double-byte characters or fields begin and end.)
ShowStatusBar		Display the status bar in Classic mode.
SubstituteDisplayChars		Specify whether zeroes should be displayed with a slash (Ø) or without a slash (0).
SupportDBCSFeatures	Misc.	Support double-byte character sets.
TelnetXSystem		Support the X SYSTEM in 3270 sessions. X SYSTEM is a keyboard locked state that occurs when the host ends a transmission to the workstation without unlocking the keyboard. Some applications use this to notify you of a message written to the display, requiring you to reset the keyboard before you can type again. Other applications rely on SNA to unlock the keyboard.
TextBlinkRate		The rate at which blinking text blinks.
TSOFileListCommand		The name of the host executable to run when, from the Transfer dialog box, the Show host files button is clicked.

Item Name	Sub-group	UI Description
TSOMemberListCommand		The name of the host executable to run when, from the **Transfer** dialog box, a member that is expanded is clicked.
TypeAhead	Input	Select to buffer characters that are typed in the terminal window. When characters are buffered, they are sent to the host as soon as possible. When characters are not buffered, anything typed while the host is not ready is lost.
UseCtrlZ		Interprets the Ctrl-Z character as an end-of-file character (when reading a file) or appends the character at the end of a file (when saving a file).
WordWrap	Input	Enable word wrap.
WordWrap3270MinimumFieldLength		Wrap text to the next available field when entered text is too long to fit in a text entry field.

5250 Items

In this Section

Permissions Manager Items: TN5250 Advanced

TN5250 Advanced

Item Name	Sub-group	UI Description
AS400Host		The name of the IBM System i host to connect to when Service Location Protocol (SLP) is enabled.
Async TransportEnabled		Revert to polling mode for host interactions. This is mainly used for diagnostic purposes.
AutoReconnect		Reconnect after a disconnection that is not initiated by Reflection.
AutoSignon	Sign-on Options	Sign-on options (all options).
BackSpaceKeyAsDelete		Treat Backspace key as Delete key.
BeforeConnectStartupMacro		Run a macro or other action before the initial connection.

Item Name	Sub-group	UI Description
ConnectMacro	Connection Action	Run a macro or other action after the initial connection.
ConnectMacroData		The name of a macro that is run automatically after a connection is established.
ConnectScript		A Reflection script that is run automatically after a connection is established.
ConnectScriptArguments		A parameter string to pass to the connect script after a connection is established.
DBCSUnmappedChar		Allows user to choose how to translate double-byte host characters that are not available in the Shift-JIS double-byte character translation table.
DefaultPorts		Attempt to communicate with the host transaction programs using the default port numbers (as defined by IBM).
FileSystem		Allow users to choose whether to use the ANSI character set or the ASCII character set for ASCII transfers from the host.
HLLAPILongName		The HLLAPI application associated with a particular Reflection session.
HLLAPIShortName		An identifier that a HLLAPI application uses to link to a Reflection session.
HLLAPIStyle	HLLAPI Options	The HLLAPI configuration. This can be a numeric value or a predefined constant.
KeepAlive	Misc.	Periodically poll the host to determine if Telnet connections remain active during intervals when you are not sending data to the host.
KeepAliveTimeout	Misc.	The interval, measured in seconds, between keep alive requests sent by Reflection.
ModeName		The properties of your application. The default value is "QPCSUPP", which is the common mode name defined on the IBM System i for 5250 applications.
MPTNIPAddress		A suffix for a fully qualified host name, with an SNA domain name suffix, either in your Hosts file or in your TCP/IP Domain Name Server.
Password	Sign-on Options	A Password (under Automatically sign on using specified user ID and password).
ReuseMSSNAPoolName		Allow users to specify how Reflection handles MS SNA pool names. When cleared (the default), administrators must assign the pool to each user for the number of connections the user needs. When selected, administrators can assign the pool once to each user.

Item Name	Sub-group	UI Description
RunMacroAtReconnect	Connection Action	Run when reconnecting.
SecurityDialog		Open the Security Properties dialog box to set up secure data communications with SOCKS or SSL/TLS.
SingleSignOn		Use a single user name and password for multiple log on procedures.
TelnetEnvironment		Automatically log on to the host as soon as a connection with Reflection is established.
TelnetLocation	Misc.	The location where the connection originated. This can also be used to provide informational messages to the host from the PC.
TNAPPNGateway		Adds the third PC Support header to the Telnet pass-through header for a save screen command, and removes it for a restore screen command. This is valid for 5250 connections over Telnet to an Apertus gateway only.
UserDataDirectory		The folder where user-created files, like settings files and trace files, are saved by default.
UserID	Sign-on Options	The user ID (under **Automatically sign on using specified user ID and password**).

Related Topics

- "Permissions Manager Items: TN5250 Basic" on page 173

Permissions Manager Items: TN5250 Basic

TN5250 Basic

Item Name	Sub-group	UI Description
AutoConnect	Connection Options	Automatically connect to the host.
ConnectionTimeout		The time period (in seconds) to wait for a host connection response.
DeviceName	Connection	The device name.
EnableConnectionTimeout		Enable or disable a connection timeout.
ExitOnDisconnect		Automatically close the session when a session is disconnected.
GenerateDeviceNames	Connection	Generate device names.
Host	Connection	The host name/IP address.
ModelID	Model	The Model ID.
Port	Connection	The Port number.

Item Name	Sub-group	UI Description
PromptReconnect		Prompt to confirm whether to disconnect a session when a session is disconnected manually or by closing the session or the workspace.
UseIDManagement		Set up ID Management. To use ID Manager, you'll need access to a centralized management server with ID Manager configured.

Related Topics

- "Permissions Manager Items: TN5250 Advanced" on page 171

Permissions Manager Items: 5250 Terminal Configuration

Item Name	Sub-group	UI Description
AIDFieldExitMode	Misc.	Enable AID field exit mode
AllowValidThaiInput		Turn off validity checking for Thai characters. (By default, when you enter Thai characters in a host application, Reflection determines whether the input is legal according to the rules of Thai character composition.)
AutoIME		Automatically turn the Input Method Editor (IME) on when the cursor is in a double-byte input field, and off when the cursor is in a single-byte input field. When it is not specified, the state of the IME does not change in response to the cursor's location.
BDTIgnoreScrollLock		Ignore the state of Scroll Lock.
C370CharSet		Use the C/370 code page. The C/370 code page provides support for square brackets ("[" and "]").
Caption		Specifies the string that appears in the Reflection title bar when running in Classic mode. This string is also displayed on the taskbar when Reflection is running.
CmdPrompt		The character or characters in the terminal window, after which Reflection attempts to insert Quick Text.
ColumnSeparator	Display	Select to use either dots or vertical lines to separate columns.
CommandLineEnabled		Specify whether the Reflection command line can be activated (for example, with the Alt-L keystroke).
CountryExtendedGraphicsCode		Select to make additional characters available in the configured National character set.

Item Name	Sub-group	UI Description
CursorMovementStyle		Specifies how the cursor moves between composed Thai characters.
CursorProgressionIndicator		Specifies how Reflection responds when the host queries to determine if End User Interface (EUI) enhancements are supported by the terminal. Use only for host applications that use cursor progression and queries to determine if EUI is supported.
DBCSUserDefinedCharacterSource		The location of user-defined character fonts.
DisplayMargins		Display margins around the terminal window.
EnableHotspots	Display	Enable all defined hotspots
EnableQuickText		Use the Quick Text feature.
EnterKeyRepeat		Specifies whether holding down the Enter key is equivalent to pressing it multiple times.
ExtendHotSpots		Treat a region to the right of a hotspot as part of the hotspot.
HorizontalCursorSpeed		Specify how many character spaces to move the cursor, either to the left (on Left Double function), or to the right (on a Right Double function).
HostBeep		Enable host beep.
HostCodePage		Host Code page.
HostControlsOutlineColor		Set the session so that the host determines the color of field outline characters. When cleared, the color of field outline characters can be configured in the Modify Theme dialog box.
HostCursorBlinkControl		Set a session so that the host controls the cursor blink rate.
HostNumlockControl		Allows the host to turn NumLock on.
HostTypeAheadControl		Honor the keyboard buffering control setting in the user IBM System i user profile.
HotspotsAltKey	Activation	Under Choose key(s) to press in combination with mouse click, activate the Alt key.
HotspotsCtrlKey	Activation	Under Choose key(s) to press in combination with mouse click, activate the Ctrl key.
HotspotsDoubleClick	Activation	Under Choose key(s) to press in combination with mouse click, activate the double-click action.

Item Name	Sub-group	UI Description
HotspotsMouseButton	**Activation**	Choose the mouse button to activate hotspots.
HotspotsShiftKey	**Activation**	Under **Choose key(s) to press in combination with mouse click**, activate the Shift key.
InputFieldUnderlines		Specify how Reflection underlines input fields on host screens.
InsertArena		Specify the extent to which the I**nsertProtocol** property applies — to a single field, across multiple local fields, or to all unprotected fields.
InsertProtocol		Specify how a character will be inserted.
KeyboardAlarmError	**Input**	Beep when keyboard error is detected.
KeyoardErrorReset	**Input**	Keyboard error.
KeysDuringWait		Specifies whether the user can use the keyboard during a synchronous command. A synchronous command (such as **Wait** or **WaitEvent**) causes a procedure to pause until a defined waiting period expires.
MappedNumlockPreservesNumlock		Specifies how Reflection behaves if a user presses the PC NumLock key when it has been mapped to emulate the action of a terminal key.
MouseShape		Specifies the appearance of the mouse pointer in the terminal window.
NumberMouseButtons		Specifies the number of buttons in the Mouse Mapper list.
PreserveEntryMode		Specifies whether Reflection remains in Extended Graphics or Hexadecimal mode indefinitely after you enter either mode. From Extended Graphics mode, you can enter multiple graphics; from Hexadecimal mode, you can enter hexadecimal characters.
QuickText		The contents of the quick text buffer.
RectangularSelection		Specify that dragging the mouse across an area selects only the text within that area. When this option is cleared (unchecked), the selection wraps to line ends.
RestrictedCursor		Restrict the cursor to input fields in the terminal window.

Item Name	Sub-group	UI Description
RightControlKeyRepeat		Designate the right Ctrl key as a modifier key. (A modifier key is used in combination with another key to send a function. For example, Ctrl-F1 is mapped to the Attention key in 3270 sessions).
ShowAttributesAsHex		Display field attributes in Hexadecimal format.
ShowBytesRemaining		Display the Show Bytes Remaining indicator on the host status line. This indicator displays the number of bytes remaining in the current field.
ShowHotspots	Display	Show all defined hotspots.
ShowMenuBar		Display the menu and toolbar in Classic mode.
ShowOIA		Specifies whether Reflection shows operation and status messages in the Operator Information Area (OIA) at the bottom of the terminal window.
ShowSOSIChars		Specifies whether to show shift-out and shift-in (SO/SI) control characters on the terminal screen. (This helps to determine where double-byte characters or fields begin and end.)
ShowStatusBar		Display the status bar in Classic mode.
StatusLine		Specifies the type of host status line for IBM System i terminals.
SubstituteDisplayChars		Specify whether zeroes should be displayed with a slash (Ø) or without a slash (0).
SupportDBCSFeatures	Misc.	Support double-byte character sets.
TextBlinkRate		The rate at which blinking text blinks.
TypeAhead	Input	Select to buffer characters that are typed in the terminal window. When characters are buffered, they are sent to the host as soon as possible. When characters are not buffered, anything typed while the host is not ready is lost.
UseCtrlZ		Interprets the Ctrl-Z character as an end-of-file character (when reading a file) or appends the character at the end of a file (when saving a file).
UserDefinedCharactersViaTelnet		Send User Defined Character (UDC) requests to the IBM System i host when you are connected through Telnet.
WordWrapAS400	Input	Enable word wrap.

Permissions Manager Items: Clipboard

Clipboard

Item Name	Sub-group	UI Description
AutoCopyOnSelect	Copy	Automatically copy selected text.
BlanksBetweenFields	Copy	Insert blanks between fields (under Use table format).
ClearSelectionOnCopy	Copy	Clear selection after copying.
ClipboardPrologue		Configure the macro recorder to add additional, language-specific code to recorded actions placed on the Clipboard.
ClipboardSyntax		The programming language used when recorded actions are placed on the Clipboard.
CopyDataSeparation		Specify whether the data copied from Reflection should be separated by delimiters at field boundaries or at word boundaries.
CopyFormatBIFF		Specifies to copy from Reflection to the clipboard in Binary Interchange (BIFF) file format.
CopyFormatDIB		Specifies to copy from Reflection to the clipboard in Device Independent Bitmap (DIB) format.
CopyFormatOptions		Specify which file formats to copy from Reflection to the clipboard.
CopyFormatRefMF		Specifies to copy from Reflection to the clipboard in the Reflection proprietary format.
CopyFormatRTF		Specifies to copy from Reflection to the clipboard in rich text format.
CopyFormatText		Specifies to copy from Reflection to the clipboard in text .txt format.
CopyFormatUnicode		Specifies to copy from Reflection to the clipboard in Unicode text format.
CopyInputFieldsOnly	Copy	Copy input fields only.
CopyTrailingSpaces	Copy	Copy trailing spaces.
CutFillCharacter	Cut	Select how you want to fill cut area — with spaces or nulls.
LimitedRTF		Specify whether to copy the font color when text is copied in rich text format.
PasteAlignText		Align space separated data with fields on the screen.

Item Name	Sub-group	UI Description
PasteClearField		Clear all of the previous data remaining in a field after pasting new data into it.
PasteIgnoreFieldType		Skips pasting text into a restricted field if the text is not a valid entry for that field and pastes remaining text into subsequent fields. This setting applies only to IBM 5250 sessions.
PasteLineBreak		The character that is actually inserted in a field on the terminal screen when data containing line breaks is copied from the Clipboard.
PasteMaskProtectedFields		Paste text into unprotected fields.
PasteMoveCursor		Specify to move the cursor to the end of the pasted text. When unselected, the cursor is restored to the position it was in before the text was pasted.
PasteReplaceTabs	Paste	The Replace tabs with option that enables the text box used to provide tab replacement.
PasteTabReplacement	Paste	The text box used to provide tab replacement.
PasteUsingFieldDelimiters	Paste	Use field delimiters.
PasteWrapDown		Wrap text to the next field below instead of the next field to the right.
PasteWrapText	Paste	Wrap text to the next input field.
RetainSelection	Copy	Retain selection.
UseTableFormat	Copy	Use table format.

Permissions Manager Items: IDManagement

IDManagement

Item Name	Sub-group	UI Description
IDMCriteria		Set the parameters required by the ID Manager server to allocate an ID, such as a pool name.
IDMPoolName		The name of a pool of resource IDs.
IDMServerURL		Specify the complete URL for the ID Management server.

Permissions Manager Items: Hotspots

Hotspots

Item Name	Sub-group	UI Description
HotspotMatchCase		Specifies the default case sensitivity for identifying hotspots.
HotspotOtherDelimiters		Allows uses of additional characters to delineate hotspots. See UseOtherDelimiters.
HotspotSpaceDelimiter		Delimits hotspots with the space character.
HotspotStyle		Defines how hotspots are displayed.
MapFile		The name of the file containing hotspots mappings.
UnprotectedFieldHotSpots		Enable hotspots in unprotected fields. (This setting does not apply to VT terminals.)
UseOtherDelimiters		Enables the use of characters defined in setting HotspotOtherDelimiters to delineate hotspots.

Permissions Manager Items: VBAReferences

Shared Macros

Item Name	Sub-group	UI Description
VBAReferences		Specifies session document files that contain macros you want to reference.

Permissions Manager Items: Document Map files

In this Section

Permissions Manager Items: Document\Classic

Classic

Item Name	UI Description
MapFile	Restrict the ability of users to modify their UI in the **Manage Ribbon** dialog box, (when operating in Classic mode).

Permissions Manager Items: Document\ClassicMDI

Classic

Item Name	UI Description
MapFile	Restrict the ability of users to modify their UI in the **Manage Ribbon** dialog box, (when operating in Classic MDI mode).

Permissions Manager Items: Document\Keyboard

Keyboard

Item Name	UI Description
MapFile	Restrict the ability of users to select or modify a keyboard map

Permissions Manager Items: Document\Mouse

Mouse

Item Name	UI Description
MapFile	Restrict the ability of users to select or modify a mouse map.

Permissions Manager Items: Document\Ribbon

Ribbon

Item Name	UI Description
MapFile	Restrict the ability of users to select or modify a Ribbon.

Permissions Manager Items: Document\QuickPads

Theme

Item Name	UI Description
QuickPadsShowTooltips	Enable tooltips on QuickPad controls.
QuickPadsToOpen	Change the QuickPads displayed in the session.

Permissions Manager Items: Document\Theme

Theme

Item Name	UI Description
MapFile	Restrict the ability of users to select or modify a theme.

Permissions Manager Items: Productivity\SpellCheck

Spell Check

Item Name	UI Description
AutoCorrect	Commonly misspelled words are corrected without prompt or indication as you type. **NOTE:** This feature is available only for English.
CheckSpellingAsType	Spell Check marks possible errors with wavy underlines.
CorrectCapsLock	If you accidentally type a word in Title Case with the CAPS LOCK key turned on, Spell Check corrects the capitalization; for example, `eNTER kEY` changes to `Enter Key`.
CorrectTwoInitialCaps	If you type two consecutive uppercase letters at the beginning of a word, Spell Check changes the second uppercase letter to a lowercase letter; for example, `ENter` changes to `Enter`.
CustomDictionary	The path to the custom dictionary file.
IgnoreAllUppercase	If you are typing in UPPERCASE letters, Spell Check does not attempt to correct spelling.
IgnoreWordsWithNumbers	If you are typing a word with a number in it, like `UrsaMajorM51`, Spell Check does not attempt to correct the spelling.
MainLanguage	The main language used for spell checking.
MaxSuggestions	The number of suggested spellings to offer when a misspelled word is encountered.
MaxWordLength	The longest word checked for spelling. Longer words are ignored by the spell checker.
MinimumMatch	The shortest field in which to check spelling.

Permissions Manager Items: Productivity

Productivity

Item Name	Sub-group	UI Description
AutoCompleteEnabled		Enable or disable the Auto Complete feature.
AutoExpandEnabled		Enable or disable the Auto Expand feature.
RecentTypingEnabled		Enable or disable the Recent Typing feature.
SpellCheckEnabled		Enable or disable the Spell Check feature.

Permissions Manager Items: Productivity\ScreenHistory

Productivity\ScreenHistory

Item Name	Sub-group	UI Description
ClearHistoryOnClose		Delete when the session is disconnected for any reason. **NOTE:** If the screen history has been saved to a file, the screen history file is not affected.
ManualCaptureOnly		Capture screens only when manual captures are performed.
MaxScreen		The maximum number of screens to record and keep at any one time in the current session's screen history.

Permissions Manager Items: Productivity\RecentTyping

Productivity\RecentTyping

Item Name	Sub-group	UI Description
ClearListOnClose		The Recent Typing list is deleted when the session is disconnected for any reason. **NOTE:** If the Recent Typing list has been saved to a file, the recent typing file is not affected.
MaxListItems		The maximum number of words to remember.
MinimumMatch		The number of characters that Reflection considers a word.

Permissions Manager Items: Productivity\Office

Productivity\Office

Item Name	Sub-group	UI Description
CloseOfficeDocs		Close Office documents when exiting Reflection. If the documents are not saved, Office prompts you to save them before closing.
PresentationTemplateFile		The default presentation template file.
WordProcessingTemplateFile		The default word-processing template file.

Permissions Manager Items: Productivity\AutoExpand

Productivity\AutoExpand

Item Name	Sub-group	UI Description
AutoExpandList		Enter the list of terms that are automatically expanded when using the Auto Expand feature
AutoExpandOverwrite		Overwrite only the data that exists where the Auto Expand definition is being placed — other data in the field is not affected.
CaseSensitive		Use case sensitivity when expanding.
ExpandAndContinue		Wrap text into next field.

Permissions Manager Items: Productivity\AutoComplete

Productivity\AutoComplete

Item Name	Sub-group	UI Description
AllScreenData		Make suggestions based on all user data that has been entered into any field used during the session.
AutoCompleteOverwrite		Overwrite only the data that exists where the Auto Complete suggestion is being placed. Other data in the field is not affected.
CaseSensitive		Use case sensitivity for suggestions.
CompleteAndContinue		If the Auto Complete suggestion pushes existing data past the end of the field, the additional data is added at the beginning of the next available field.
MaxSuggestions		The maximum number of items you want Auto Complete to suggest for any word.
MaxWordLength		The longest word on which to apply Auto Complete. Longer words are ignored.

Item Name	Sub-group	UI Description
MinimumMatch		The number of characters typed before suggestions are made.
PersistData		Auto Complete "remembers" the data entered during the current session, so that if the session is closed, and then reopened, suggestions will still be available.

Permissions Manager Items: Application Workspace

In this Section

Permissions Manager Items: Application Access\API Security

API Security

Item Name	Sub-group	UI Description
ChannelType		Prevent custom applications from accessing Reflection.
LegacyCOM		The legacy API used for the GetObject() method to retrieve API COM objects — No Legacy API, Reflection, or Extra!.
RequiredUACForRestrictedAction		Require UAC elevation when a restricted action is invoked by a macro or API call.

Permissions Manager Items: Application Access\Application Options

Application Options

Item Name	Sub-group	UI Description
ApplicationStartup		Specifies which dialog box, if any, to display when Reflection starts.

Item Name	Sub-group	UI Description
ClearClipboardOnExit		Any data that may have been copied to the Clipboard is cleared when the workspace is closed.
CustomHelpSystemURL		The URL to use for Help.
DefaultSettingsLocalPath		The path for the default directory in which session and other documents are saved.
ExitOnLastDocumentClose		Automatically exits the workspace when the last document in the workspace is closed.
HelpSystem		Specify whether to use the product Help as it appears on the Micro Focus Web site or the Help installed on your local machine.
HideBuiltInTemplates		Display only user-defined templates from the Create New Document dialog box.
HLLAPILogFile		Set the log file that HLLAPI traces are saved in.
HLLAPILogging		Select to enable HLLAPI logging to the specified file.
Logging		Send error information to the Windows logging service.
MacroSearchPath		Change the default directory in which to save Extra! macros or legacy files, such as QuickPads.
OpenDocumentsInSameWorkspace		Specify that when sessions are opened by double-clicking on session document files, the sessions all open in the same workspace.
OptimizeRemoteSession		Turn off cursor blinking and disable the splash screen when running Reflection under Citrix or WTS. **NOTE:** This setting is ignored if you are not running under Citrix or WTS;
PromptForDisconnect		Prompt to confirm whether to disconnect a session when a session is disconnected manually or by closing the session or the workspace.
SaveSessionAsCompoundDocument		Save a session in a file format that includes all configuration files (keyboard maps, etc) in a single file.
SessionShutdown		Specify what you want done with any changed settings when you close a document.
StartupAction		Set up an action (for example, a startup macro) that is performed when Reflection starts.
UsageDataEnabled		Allow the product to gather and send information about how the software is used.

Permissions Manager Items: Application Access\Application Sounds

Application Sounds

Item Name	Sub-group	UI Description
Events		Map events to sound files.

Permissions Manager Items: Application Access\Centralized Management

Centralized Management

Item Name	Sub-group	UI Description
AuthenticationRequired		Require users to log on to a centralized management server to use Reflection.
AutomatedSignOnForMainframeEnabled		Enables automated sign-on for sessions that are not managed by the centralized management server.
CentralizedManagementEnabled		Allow the workspace to download and run sessions from the centralized management server.
CentralManagementServerUrl		Specify the URL of the server used to centrally manage sessions.
CertificateManagementEnabled		Require user sessions to pull certificates from a centralized management server.

Permissions Manager Items: Application Access\HLLAPISettings

HLLAPI Settings

Item Name	Sub-group	UI Description
Associations		Does not apply to Reflection.
IHLLAPIWorkspaceVisible		Does not apply to Reflection.
ShortNames		Does not apply to Reflection.

Permissions Manager Items: Application Access\InfoconnectPathManager

Path Manager

Item Name	Sub-group	UI Description
ManagePath		Does not apply to Reflection.

Permissions Manager Items: Application Access\PCI DSS

PCI DSS

Item Name	Sub-group	UI Description
APIsReadRedacted		Allow programs or macros using the Reflection .NET and VBA APIs to read redacted data as clear text.
ConnectionToUseSecureProtocol		Specify whether to require secure connections. Security can be required for all connections or for only wireless connections.
CopyUnredacted		Allow users to copy redacted data from a screen in an IBM session to another screen in the same session or to a screen in another IBM session.
ExceptionRegularExpressions		Define exception expressions that filter out false PAN detections. These only apply when the Reflection PAN detection method is used.
NeedRaiseEvent		Specify whether API events occur when a user views a credit card Primary Account Number (PAN).
PrecedingKnownStrings		Define a list of text keywords that precede PANs. These apply only when the Detect PANs based on preceding text method is selected.
RecognitionStyle		Specify which type of PAN Detection to use.
RedactionRules		Choose to redact data on the screen after it is entered or as it is typed.
RedactStyle		Specify how many digits of the PAN to redact.
RegularExpressions		Define additional detection rules with regular expressions. These only apply when the Reflection PAN detection method is used.
RetainRedactedDataFormatting		Removes non-digit characters from a redacted string when it is pasted onto another screen.
StoreTypedPANs		Determine whether or not PAN data are stored.

Permissions Manager Items: Application Access\Privacy Filter

Privacy Filter

Item Name	Sub-group	UI Description
MapFile		The list of privacy filters.
Redaction Rules		Specify how data affected by Privacy Filters will be redacted.

Permissions Manager Items: Application Access\TrustedLocations

TrustedLocations

Item Name	Sub-group	UI Description
AllowNetwork		Permit network paths to be included in the list of trusted locations. **NOTE:** This is not recommended.
TrustAllLocations		Open files only from trusted locations.
TrustedLocations		The list of trusted locations.

Permissions Manager Items: Application Access\UX Configuration

UX Configuration

Item Name	Sub-group	UI Description
CloseButtonOnTab		Specifies to display a Close button on each document tab.
DocumentLayout		Specifies how to display documents in the workspace — using tabs (the default), or as windows that you can tile or cascade.
Language		The language you want to use for the UI — the menus, dialog boxes, and Help when you start a new session.
MaxRecentDocuments		The maximum number of recently used documents to display in the Recent Documents list on the "Reflection Workspace menu" on page 897.
ShowDocumentSwitcher		When selected, pressing the Ctr+Tab displays a document switcher that can be used to tab through the open documents.
ShowHelp		Displays the Help icon and menu on the Ribbon.

Item Name	Sub-group	UI Description
ShowQuickAccessToolbar		Displays the Quick Access Toolbar on the Ribbon or Browser.
ShowSearch		Displays the Search box on the workspace.
ShowStartPage		Displays a gallery of recent documents.
ShowSuggestion		Displays search suggestions when you type in the Search box. (This applies only to Browser mode.)
SuppressRibbonTooltipFooter		Select to hide the F1 Help link that is displayed on tooltips by default.
SuppressTooltips		Select to hide tooltips on the ribbon, the status bar, and the Macro Panel.
TabStripLocation		Where to display the document tabs — at the top (default), bottom, left, or right.
UseAlternateIcons		Specifies whether to use modern, "flat" toolbar icons or the older toolbar icons used on previous versions of Reflection.
WindowLookAndFeel		The user interface mode— Ribbon, (the default), Browser, Classic, Classic MDI, or TouchUx.
WindowTheme		The color scheme to use.

Permissions Manager Items: VT terminal

In this Section

Permissions Manager Items: VT Terminal\Document\Clipboard

Document\Clipboard

Item Name	Sub-group	UI Description
CopyDataFormat		Specifies how to format data that is copied from Reflection to the clipboard.
CopyTableMethod		Specifies whether to detect columns using vertical spaces and whether to convert two or more spaces to tabs when data is copied.
PasteBufferSize		The size of a "paste block," which is the number of characters pasted from the Clipboard to the terminal window before a pause occurs.
PasteDelay		The time interval (in tenths of a second) that Reflection waits between "paste blocks" when pasting data from the Clipboard into display memory.
RetainDisplayFormat		Retains formatting when data is copied from the terminal screen.

Permissions Manager Items: VT Terminal\Document\Connection

Document\Connection

Item Name	Sub-group	UI Description
AutoConnect		Specify to establish a host connection as soon as the associated session document is opened.
AutoReconnect		Specify to attempt to reestablish the connection when the session is disconnected
Baud		The rate at which Reflection transmits and receives data through the selected serial port.
BeforeConnectStartupMacro		Run a macro before the initial connection.
ConnectionMethod		Determines how the session connects to the host (Network, Serial Port, Modem). This setting is used in conjunction with ConnectionType.
ConnectionType		Determines how the session connects to the host (Telnet, Secure Shell, Rlogin). This setting is used in conjunction with ConnectionMethod.
ConnectMacro		Run the connection action when the session initially connects to a host.
ExitAllowed		Specify to allow closing the workspace when a session is connected to a host.
ExitOnDisconnect		Specify to automatically close the session when a session is disconnected.

Item Name	Sub-group	UI Description
Host		The name of the host to which to connect.
ModemAdvancedSettingsDialog		The **More Settings Modem** dialog box. Restricting access to this setting limits user access to this dialog box when a session is configured for a modem connection.
ModemAreaCode		The area code (or city code) of the number being dialed.
ModemCountryName		The country of the number being dialed.
ModemDialingPropertiesDialog		The **Phone and Modem Options** dialog box. Restricting access to this setting limits user access to this dialog box when a session is configured for a modem connection.
ModemLocation		The current modem location. Modem locations are configured using the Control Panel tool.
ModemName		The type of modem being used.
ModemPhoneNumber		The phone number you want the modem to dial when connecting. The number must adhere to the rules of your modem.
ModemUserDialingRules		Set the TAPI modem dialer to add appropriate dialing prefixes to the number you are dialing, based on the current values of **ModemAreaCode**, **ModemCountryName**, and **ModemLocation**. When cleared, the modem dialer dials the phone number exactly as specified by **ModemPhoneNumber**.
NetworkAdvancedSettingsDialog		The **More Settings -** *Network* dialog box. Restricting access to this setting limits user access to this dialog box when a session is configured for a network connection.
NetworkSecurityDialog		The **Security Properties** dialog box. Restricting access to this setting limits user access to this dialog box when a session is configured for a network connection.
Parity		The parity for data transmission to and from the serial device on this port. To use the multinational character set or 8-bit controls, **Parity** must be set to one of the values that offers 8-bit controls. If your communications link generates parity, and you set **Parity** to **8/None**, multinational characters appear on your screen. In this case, set **Parity** to either **8/Even** or **8/Odd**.

Item Name	Sub-group	UI Description
Port		The host port or socket number that the session should use.
		This item restricts access to the Port setting when a Telnet connection type is selected. To restrict access when the Rlogin connection type is selected, use the RloginPort item.
PromptReconnect		Prompt to confirm whether to disconnect a session when a session is disconnected manually or by closing the session or the workspace.
RloginPort		The host port or socket number that the session should use when using an Rlogin connection.
		This item restricts access to the Port setting when an Rlogin connection type is selected.
RunMacroAtReconnect		Run the macro when the session initially connects to a host, and every time it reconnects to the host.
SerialAdvancedSettingsDialog		The More Settings - Serial Port dialog box. Restricting access to this setting limits user access to this dialog box when a session is configured for a Serial Port connection.
SerialPort		The serial port to use when connecting to the host via a serial port connection.
SSHConfigScheme		The SSH configuration scheme settings to use to make a Secure Shell connection.
SSHSingleSettings		Does not apply to Reflection.
SSHTermWindowAuth		Set up Secure Shell connections to display user name and password prompts in the terminal window instead of in a dialog box.
UserName		A name that identifies you or your PC to the host.

Permissions Manager Items: VT Terminal\Document\Terminal

Document\Terminal

Item Name	Sub-group	UI Description
AutoResizeScreen		Automatically resize the terminal window to accommodate the data being displayed.
Caption		Specifies the string that appears in the Reflection title bar when running in Classic mode. This string is also displayed on the taskbar when Reflection is running.
		NOTE: This item applies to the Window title setting.

Item Name	Sub-group	UI Description
CompressBlankLines		Specify whether to save room in display memory by compressing multiple blank lines into a single blank line.
DisplayColumns		Display the number of columns in the complete terminal display.
DisplayMemoryBlocks		The number of 8K memory blocks to allocate for display memory.
DisplayRows		Display the number of rows in the complete terminal display.
EnableHotspots		Enable all defined hotspots.
GraphicsTerminal		Emulate a graphics terminal.
HotspotsAltKey	**Activation**	Under **Choose key(s) to press in combination with mouse click**, activate the Alt key.
HotspotsCtrlKey	**Activation**	Under **Choose key(s) to press in combination with mouse click**, activate the Ctrl key.
HotspotsDoubleClick	**Activation**	Under **Choose key(s) to press in combination with mouse click**, activate the double-click action.
HotspotsMouseButton	**Activation**	Choose the mouse button to activate hotspots.
HotspotsShiftKey	**Activation**	Under **Choose key(s) to press in combination with mouse click**, activate the Shift key.
JumpScrollSpeed		Control the screen refresh frequency.
MouseCursorShape		Specify whether to display the mouse cursor as an i-beam or an arrow.
MultiplePageTerminal		Emulate a multi-page terminal.
NewPageOnClear		Clear the data on the display when you or the host clear the display.
SaveFromScrollingRegion		Move text that scrolls out of the scrolling region into display memory.
ShowControlCharacters		Display control characters. This lets you see exactly which characters are received from the host and which control characters are generated by the keyboard.
ShowHotSpots		Specify to display hotspots as buttons.
ShowMenuBar		Display the menu and toolbar in Classic mode.
ShowStatusBar		Display the status bar in Classic mode.
SmoothScroll		The scroll speed setting.

Item Name	Sub-group	UI Description
TerminalAdvancedSettingsDialog		The Terminal Setup dialog box. Restricting access to this setting limits user access to this dialog box.
TerminalType		The type of terminal to emulate (VT500-7, XTERM, WYSE, and so on).
WyseLabelLines		The number of label lines that are visible. This property is valid only during Wyse terminal emulation.

Permissions Manager Items: VT Terminal\Document\Safeguards

Document\Safeguards

Item Name	Sub-group	UI Description
CacheSecureShellUserName		Temporarily stores the user name entered for a Secure Shell session until the Reflection workspace is closed. (When selected, users are not prompted for a user name when they reconnect unless they reopen the workspace.)
ClearDisplayOnDisconnect		Delete all data from display memory when a session is disconnected from the host.
SaveSecureShellUserName		Save the user name when users save their settings files, or record a macro.

Permissions Manager Items: 6530 terminal

Permissions Manager Items: 6530 Terminal\Document\Clipboard

This group controls settings in the Configure Clipboard Settings dialog box accessed from the Settings window in a 6530 session.

Item Name	Sub-group	UI Description
CopyInputOptions		Add tabs between fields and Truncate trailing spaces
		These two settings specify behavior when performing a Copy Input menu ribbon function, which copies only unprotected fields on a block mode screen into the clipboard:
		Add tabs between fields places tab characters between the fields.
		Truncate trailing spaces removes trailing spaces from each field.
PasteMapEnabled		**Map carriage return, line feed to tab**
		When pasting, replaces any carriage return and line feed characters with a single tab character.
PasteTabCount		**Number of spaces**
		When **Replace tabs with spaces** is selected, any tabs in the pasted data are converted into the number of spaces specified in this field
PasteTabEnabled		**Replace tabs with spaces**
		When selected, the Number of spaces field becomes available, and any tabs in the pasted data will be converted into the number of spaces specified in the **Number of spaces** field.
SelectType		**Line** and **Rectangle**
		Line text selection wraps from the end of one line to the beginning of the next.
		Rectangle text selection does not wrap across line boundaries but instead the left and right edges of the selected area fall in the same column on every line.

Permissions Manager Items: 6530 Terminal\Document\Connection\Security

This group controls settings in the Set Up Connection Security dialog box accessed from the Settings window in a 6530 session.

Item Name	Dialog box	UI Description
SSHEnabled	Set up Connection Security	**Use SSH** Specifies to use SSH for Authentication/Encryption and allows you to use the **Configure SSH** button to open the Configure SSH Security dialog box.
SSLEnabled	**Set up Connection Security**	**Use SSL/TLS** Specifies to use SSL/TLS for Authentication/ Encryption and allows you to use the **Configure SSL/TLS** button to open the Configure SSL/TLS Security dialog box.

Permissions Manager Items: 6530 Terminal\Document\Connection\Security\SSH

This group controls settings in the Configure SSH Security dialog box accessed from the Settings window in a 6530 session.

Item Name	Sub-group	UI Description
sshAuthenticationGSSAPIEnabled		**Use GSSAPI** uses GSSAPI for authentication (User name and Password and/or keys are not required).
sshAuthenticationKeyboardInteractiveEnabled		**Keyboard interactive** When this option is selected, the host prompts for the User name and Password.
sshAuthenticationPasswordEnabled		**Password** under **User Authentication** The password is entered in this box when using User name and Password only to authenticate.
sshAuthenticationPublicKeyEnabled		**Public Key** uses keys only to authenticate.
SSHBannerWindow		**Banner window** specifies for the greeting message from the host to appear in a separate window instead of on the emulation screen.
SSHCompression		**Compression** specifies the compression level to use.
SSHConfiguredCommand		**Execute Command** Allows you to enter a command to execute as a startup option. The session will connect, run the command, and close the connection.
SSHEncryption		**Encryption** specifies the encryption strength.

Item Name	Sub-group	UI Description
SSHHostCheck		**Host Check** specifies criteria for accepting connections. If set to No, all connections are accepted. If set to Yes and the host is not known, then the connection is refused. If set to Ask User, if the host is not yet known the user is prompted as to whether to accept the connection, and whether or not to trust this host in the future.
SSHLogging		**Enable logging** specifies to log the session to SSHLog.log in the user configuration directory.
SSHPortForwardingDefaultPort		**Port** specifies the port to forward connections to.
SSHPortForwardingEnabled		**Use port forwarding** forwards the connection to the host through the SSH server to the port specified in the **Port** field.
SSHProgramDefault		**Run Program** allows you to enter a program to run on connection. The session will connect, run the program, and when you exit the program, close the connection.
SSHSFTPEnabled		**Use SFTP** enables secure file transfers via SSH (SFTP) when using the built-in FTP client.
SSHShellDefault		**Default Shell** specifies that you will get the default UNIX shell on the system you are connecting to.
SSHStartupOption		**Startup Options** includes the Default Shell, **Execute Command**, and **Run Program** connection options.
SSHTimeoutDefault		This is the box under **Enable inactivity timeout**. It allows you to change the default timeout value.
SSHTimeoutEnabled		**Enable inactivity timeout** specifies to use a timeout. If unselected, the inactivity timeout is disabled.
SSHUsername		**User name** specifies the user name on the SSH host. A user name is required for all authentication methods.
SSHUserPassword		**Password** under **User Authentication** The password is entered in this box when using User name and Password only to authenticate.
SSHUserPrivateKeyFile		**Private key file** allows you to enter a private key path and file name.

Item Name	Sub-group	UI Description
SSHUserPrivateKeyPassword		**Private key password** allows you to enter the password for a private key file.

Permissions Manager Items: 6530 Terminal\Document\Connection\Security\SSL

This group controls settings in the Configure SSL/TLS Security dialog box accessed from the Settings window in a 6530 session.

Item Name	Sub-group	UI Description
SSLClientCertificateEnabled		**Provide client certificate** specifies to send the client certificate in the **Client certificate file** box to the host.
SSLClientCertificateFile		**Client certificate file** specifies the client certificate filename and path.
SSLClientCertificatePassword		**Client certificate password** allows you to enter the password for the client certificate.
SSLFTPSEnabled		**Use FTPS** allows you to use FTPS to secure FTP sessions using the built-in FTP client.
SSLFTPSPort		**Port** is the port number to use for FTPS sessions using the built-in FTP client.
SSLLogging		**SSL/TLS Logging** specifies whether or not to do diagnostic logging of the session, and what level of logging should be done.
SSLServerAuthentication		**Server Authentication** includes the following settings:
		Check for valid CA signature checks the SSL/TLS Certificate to verify that it has a valid CA signature.
		Certificate host name must match host being contacted specifies that the host name in the certificate matches the host name you are connecting to.
		Perform CRL check checks the certificate against a Certificate Revocation List, and if the certificate has been revoked, the connection fails.

Permissions Manager Items: 6530 Terminal\Document\Connection\TN6530Advanced

This group controls settings in the Configure Advanced Connection Settings dialog box accessed from the Settings window in a 6530 session.

Item Name	Sub-group	UI Description
AutoReconnectInterval		**Reconnection Interval** specifies the amount of time, in seconds, to wait before another attempt to connect is made.
BlockModeBigScreen		**Block Mode** sets the number of rows and columns to use while in block mode.
ConnectMacroName		**Select Macro** under **Run a macro after the initial connection** allows you to select the name of the macro to run after the initial connection.
ConnectMacroRun		**Run a macro after the initial connection** allows you to select a macro to run after the connection has completed.
ConnectTimeout		**Connection Timeout** specifies the maximum amount of time, in seconds, to wait for a connection to the remote host to complete.
ConversationalModeScreenSize		**Conversational Mode** is used to set the size of the screen in rows and columns while in conversational mode.
FTPPort		**FTP Port** sets the port to use for FTP sessions using the built-in FTP client.
KeepAlive		**Send Keep Alive packets** enables Keep Alive messages. Keep Alive sends a packet to the host periodically to determine if the connection is still open.
ReconnectMacroRun		**Run when reconnecting** runs the macro defined to run after the initial connection when re-connecting.
ScreenColumns		**Columns** specifies the number of columns in Conversational mode when defining a custom screen size.
ScreenRows		**Rows** specifies the number of rows in Conversational mode when defining a custom screen size.
StartUpMacroName		**Select Macro** under **Run a macro before the initial connection** allows you to select a macro to run before the connection is attempted.

Item Name	Sub-group	UI Description
StartUpMacroRun		**Run a macro before the initial connection** specifies to run a macro before the connection is attempted.
TCPTrace		**Enable TCP/IP Trace** traces all TCP/IP traffic for this session.

Permissions Manager Items: 6530 Terminal\Document\Connection\TN6530Basic

This group controls settings in the Configure Connection Settings dialog box accessed from the Settings window in a 6530 session.

Item Name	Sub-group	UI Description
AlternateHostsEnabled		**Enable Alternate Hosts (Load Balancing)**
		Alternate hosts are used. Fields are displayed for entering host names and ports.
AutoConnect		**Automatically connect to the host**
		The session connects to the host as soon as it is opened.
AutoReconnect		**Automatically reconnect when connection is lost**
		If the session is lost for any reason, the session automatically reconnects.
Host		**Host name /IP address**
		The host name of IP address of the host you want to connect to.
LineModeSuppress		**Use Line Mode**
		Line mode is used. Uncheck if you wish to run in character mode. Line mode should always be used for connections to Guardian sessions on a NonStop host.
Port		**Port**
		The port number that the Telnet server listens on here. The default is the "well known" telnet port number 23.
Service		**Service**
		The service name (i.e. TACL or any other service that has been defined on this telnet server), or the name of a window that has been defined on this telnet server.

Permissions Manager Items: 6530 Terminal\Document\Input Devices\AID

This group controls settings in the Configure Alternate Input Devices dialog box accessed from the Settings window in a 6530 session.

Item Name	Sub-group	UI Description
AidAction		**Read completion action** specifies the action to take after a successful AID read. Valid choices are **None**, **TAB**, **ENTER**, or any NonStop function key.
AIdAudibleAlert		**Enable audible alert** specifies whether the bell sounds after a successful read of the Alternate Input Device.
AidBaudRate		**Baud rate** specifies the speed the serial port operates at.
AidDataBits		**Data bits** specifies the number of data bits in each character.
AidEnabled		**Use alternate input device** enables the Alternate Input Device.
AidParity		**Parity** specifies the type of parity bit added to each character.
AidPort		**Async Port** specifies the serial port to be used for the Alternate Input Device connection.
AidStopBits		**Stop bits** specifies the number of stop bits added to each character.
AidTerminationCharacter		**Termination character** specifies the terminating character that the 6530 emulation expects to see at the end of the transmission from the AID. The AID device must be configurable to send one of these characters at the end of its transmission for proper operation.

Permissions Manager Items: 6530 Terminal\Configuration\DisplaySettings

This group controls settings in the Set Up Display Settings dialog box accessed from the Settings window in a 6530 session.

Item Name	Sub-group	UI Description
BlinkingRate		**Blink rate** The speed at which the blink occurs.

Item Name	Sub-group	UI Description
BlinkingText		Display blinking text
		Fields marked as blinking by the host blink.
DisplayDelay		Display delay
		Sets the delay period between receipt of characters and updating of the display. The higher the value is, the longer the delay. For the Telnet access method this is best left at 1.
DisplayUnderline		Display underline
		Specifies whether the monochrome underline attribute is displayed.
DisplayVerticalScrollBar		Display Vertical Scroll Bar
		Displays a vertical scroll bar on the right side of the emulation screen, allowing you to move through display memory.
HostColorChangesEnabled		Allow host color changes
		Specifies whether the 6530 emulation changes the color map when the host sends color change escape sequences. Unselect this item if you prefer your own color mapping.
InvisibleMapping		Allow invisible mapping
		Specifies how the invisible attribute is displayed. If checked, invisible attribute fields are visible and therefore can be used to display more colors on the screen. If unchecked, invisible attribute fields are invisible.
Line25ExtraInfo		Line 25 Extra Information
		Specifies what is displayed on the far right side of the status line (line 25): nothing, the response time, or the cursor location.
ScrollingSpeed		Scrolling speed
		Specifies how many lines of data the 6530 emulation receives before forcing the on-screen display to be updated when it is receiving large amounts of data. Higher values result in faster scrolling.

Item Name	Sub-group	UI Description
UnderlineSpecial		Underline special
		Specifies how the underline attribute is displayed.

Permissions Manager Items: 6530 Terminal\Document\Productivity\RecentTyping

This group controls settings in the Configure Recent Typing dialog box accessed from the Settings window in a 6530 session.

Item Name	Sub-group	UI Description
ClearListOnClose		Clear recent typing list when disconnected
		Specifies that all saved recently typed items are discarded.
MaxListItems		Maximum number of items in recent typing list
		Sets the number of commands to retain in the recent typing file.
MinimumMatch		Minimum size of item in recent typing list (characters)
		Sets the smallest command to retain in the recent typing file.
RecentTypingCaptureBlockMode		Block mode capture
		Specifies that fields that are typed into are also stored as recent typing.
RecentTypingCaptureConvMode		Conversational mode capture
		When selected, commands are recorded, and the Inline Editing item is enabled.
RecentTypingCaptureOSSMode		OSS mode capture
		When selected, commands are recorded, and the Inline Editing item becomes enabled.
RecentTypingContextLoadSave		Load/save recent typing list on startup/exit
		Saves and loads the recent typing list on startup and exit.

Item Name	Sub-group	UI Description
RecentTypingEditorConvMode		**Inline editing** for **Conversational mode capture** The inline editor appears when a character is typed or the up or down arrow is pressed while at a command prompt.
RecentTypingEditorOSSMode		**Inline editing** for **OSS mode capture** The inline editor appears when a character is typed or the up or down arrow is pressed while at a command prompt.
RecentTypingEnabled		**Capture recent typing** Enables recent typing.

Permissions Manager Items: 6530 Terminal\Document\Terminal\Configuration\6530

This group controls settings in the Configure Terminal Settings dialog box accessed from the Settings window in a 6530 session.

Item Name	Sub-group	UI Description
BellColumnDefault		**Bell column** The bell column number.
BellColumnEnabled		**Enable bell column** If **Enable Beep** is selected, the margin bell rings at the column specified in the **Bell Column** field.
BellVolume		**Enable beep** If selected, anything that causes a bell causes an audible alert. This includes receiving a bell character from the host, or a margin bell if it is enabled.
EnterFunctionKey		**Use enter key as a function key** Treats the Enter key as an extra function key in block mode.
EuroEnabled		**Host supports Euro symbol**
FirmwareLevel		**Firmware revision** Specifies a three character string which identifies the firmware revision of the terminal being emulated.

Item Name	Sub-group	UI Description
HllapiId		**HLLAPI Short name**
		The HLLAPI short name of the session. Valid values are A to Z.
HllapiLongName		**HLLAPI Long name**
		The HLLAPI long name of the session.
HotSpotsEnabled		**Enable hot spots**
		Turns hot spot processing on and off.
Language		**Language** specifies the national character set used for communications with the Host computer.
LineDrawingSubstitution		**Enable line drawing character substitution**
		Replaces foreign characters with line drawing characters.
MaxPages		**Memory pages**
		Defines the number of scroll back pages that are available for data that has scrolled off the screen. Default value should be 12, and the maximum value is 400.
PFkeySupport		**Enable PF key support**
		Specifies whether or not the emulator supports PF keys.
TermId		**Terminal ID**
		Specifies the character used to identify the exact terminal type being emulated.
TypeAhead		**Enable type ahead**
		Specifies whether the emulator buffers keystrokes when the keyboard is locked, or when data is received from the NonStop.
UpshiftData		**Convert input to upper case**
		Specifies that all input typed in at the keyboard is forced to upper case, regardless of the state of the shift or caps lock keys.

Permissions Manager Items: 6530 terminal\Document\Theme

This group controls settings in the Manage Themes dialog box accessed from the Settings window in a 6530 session.

Item Name	Sub-group	UI Description
BorderColorCustom		**Guardian mode**
		Sets the border color to use while in Guardian mode.
BorderColorUseDefault		**Use default border color**
		When selected, if the emulation screen has a border, the border has the background color of the Normal attribute.
BorderOSSColorCustom		**OSS Mode** button
		Sets the border color to use while in OSS (vt220) mode.
ColorAttributes		**Terminal attribute table**
		Allows you to change the color of a terminal attribute, such as underlined text.
ColorShadesItem		**Terminal color table**
		Allows you to change the color of a specific color in the new Tandem 6530 terminal extended color escape sequences.
CursorStyleBlinkItem		**Enable cursor blink**
		Sets the cursor to blink.
CursorStyleShapeItem		**Shape**
		Allows you to select either a block or line style cursor.
FontAutoSize		**Automatically adjust font size to fit window**
		When selected, the font size automatically adjusts when the size of the window changes. If unchecked, the **Specify font size** field is available, and the font size no longer changes when the window size changes.
FontFaceName		**Font**
		The font to use.

Item Name	Sub-group	UI Description
FontPointSize		Specify font size
		Specifies the font size when **Automatically adjust font size to fit window** is unchecked.
GuardianMode		Guardian Mode
		Sets the background color while in Guardian (6530) mode.
OSSModeColors		OSS Mode Colors
		Sets the base attribute colors to use in OSS mode.
UseClearTypeFont		Use ClearType font
		When selected, the font is smoothed using ClearType, making it easier to read.

Permissions Manager Items: Security

Security\Firewall

These settings are available from the Reflection FTP client. To get to these settings, open an FTP client settings file and click **Security** on the Connect to FTP Site dialog box or create a new FTP client settings file and on the Login Information panel, click **Security**. Then in the Security Properties window side menu, select **Firewall**.

Item Name	Sub-group	UI Description
Password authentication		This setting is available when **Style** is set to username@servername. If your firewall is set up to authenticate the user prior to opening a connection to an FTP server, select this check box.If you have selected a firewall style that requires authentication, this option is selected automatically and you cannot change it.
Save password		Saves the string entered in the **Password** box as obfuscated text in your FTP settings file.
Server name		Specifies the name of the firewall that you use to log onto an FTP server.
Style		The FTP Client sends different commands for logging onto a firewall and connecting to an FTP server based on the server style you specify.
Use firewall		Enables connections through a firewall. You must select this check box before you can set other items.
User name		Specify a valid user name registered on the firewall server. For case-sensitive servers, you must use the appropriate case.This setting is unavailable if Style is set to username@servername and the Password authentication check box is cleared.

Permissions Manager Items: Security\PKI

These settings are available in the PKI section of the Secure Shell Settings dialog box.

Item Name	Sub-group	UI Description
Certificate host name must match host being contacted		Specifies whether host name matching is required when validating host certificates.
Client Authentication		Specifies whether to find a certificate for authentication or use a particular certificate.
Reflection Certificate Manager button		Opens the Reflection Certificate Manager.
Retrieve and validate certificate chain		Specifies whether certificates presented for host authentication are checked to determine if they are valid and signed by a trusted CA.
Use CRL		Specifies whether your client session checks for certificate revocation using CRLs (Certificate Revocation Lists) when validating host certificates.

Item Name	Sub-group	UI Description
Use OCSP		Specifies whether your client session checks for certificate revocation using OCSP (Online Certificate Status Protocol) responders when validating host certificates.
View System Certificates button		Opens the Certificates dialog box, which you can use to manage certificates in your system stores.

Security\Proxy

These settings enable proxy use for Reflection Secure Shell sessions. These settings are available in the Proxy section of the Secure Shell Settings dialog box.

Configure button		Configure proxy server settings.
Proxy type		Select to configure a Secure Shell connection through a SOCKS or HTTP proxy.
Use proxy server		Enable proxy use for Reflection Secure Shell sessions.

Security\SSH\Encryption

These settings specify what ciphers the Secure Shell connection should use. Different options are available depending on which Secure Shell protocol is used for the connection. These settings are available in the Encryption section of the Secure Shell Settings dialog box.

Cipher list		Specifies the ciphers you want to allow for protocol 2 connections to the current host.
HMAC list		Specifies the HMAC (hashed message authentication code) methods you want to allow. This hash is used to verify the integrity of all data packets exchanged with the server.
Key exchange algorithms		Specifies which key exchange algorithms the client supports, and the order of preference.
Run in FIPS mode		Specifies that all connections are made using security protocols and algorithms that meet FIPS 140-2 standards.

Security\SSH\General

These settings are available in the General section of the Secure Shell Settings dialog box.

Enable compression	Specifies for the client to request compression of all data. Compression is desirable on modem lines and other slow connections, but will only slow down response rate on fast networks.
Enable server keep alive	Specifies to sends NOOP messages to the server through the secure tunnel at the specified interval. Use this setting to maintain the connection to the server. Use Interval to specify how frequently server alive messages are sent.
Logging level	Determines how much information is written to the Secure Shell log file.
Port number	Specifies the port to connect to on the server. The default is 22, which is the standard port for Secure Shell connections.
Reuse existing connection if available	Specifies that multiple sessions for the same host reuse the original Secure Shell connection, and therefore don't require re-authentication. If you clear this setting, Reflection establishes a new connection for each session, which means that each new connection repeats the authentication process.

Security\SSH\Host Authentication

Use the Host Authentication section to manage the keys that authenticate the host to your client session. You can view the list of trusted hosts, add or delete host keys, and specify how you want Reflection to handle unknown hosts. These settings are available in the Host Authentication section of the Secure Shell Settings dialog box.

Delete trusted host key button	Deletes a host key from the Trusted Host Keys list.
Enforce strict host key checking	Specifies how Reflection should handle host key checking when connecting to an unknown host.
Import trusted host key button	Imports a host key.
Prefer SSH keys over certificates	Specifies the order of preference for host key algorithms. When this setting is unselected (the default), Reflection requests host certificates before host keys. When this setting is selected, Reflection requests host keys before host certificates.

Security\SSH\Host Data

Use the Host Data section to set environment variables and run commands on the server. These settings are available in the Host Data section of the Secure Shell Settings dialog box.

Add environment variable button	Opens the New Environment Variable dialog box, from which you can specify a new variable and value.
Delete environment variable button	Deletes the selected variable.
Edit environment variable button	Opens the Edit Environment Variable dialog box, from which you can edit the selected variable.
Remote command button	Specifies one or more commands to run on the remote server.

Security\SSH\Multi-Hop

Use multi-hop connections when you need to establish secure connections through a series of Secure Shell servers. These settings are available in the Multi-hop section of the Secure Shell Settings dialog box.

Add > multi-hop server button	Opens the Configure Multi-hop Server (page 479) dialog box, from which you can add a new server to the list.
Edit multi-hop server button	Opens the Configure Multi-hop Server dialog box, from which you can modify the configuration of the selected server.
Delete multi-hop server button	Deletes the selected server.

Security\SSH\SFTP

The Secure Shell section of the Security Properties dialog box is visible only if you are running the FTP Client. To get to these settings, open an FTP client settings file and click Security or create a new settings file and on the Login Information panel, click Security. Then in the Security Properties window side menu, select Secure Shell in the side menu and select Use Reflection Secure Shell.

Configure button	Opens the Reflection Secure Shell Settings dialog box, from which you can configure additional Secure Shell settings.
FTP host is different than Secure Shell host (Tunnel)	Specifies to forward all FTP communications securely through the Secure Shell tunnel to the specified Secure Shell server, then in the clear from the Secure Shell server to the FTP server.
Local port (Tunnel)	Deletes the selected server.
Preserve timestamps and file attributes (SFTP)	Specifies that files transferred to and from the server retain their date, time, and file attributes. This setting affects SFTP connections.
Send Window Size Buffer size (SFTP)	Allows you to set buffer size to improve transfer speed. The optimum values depend on your network and server setup. Changing these values may also affect how quickly you can cancel a transfer.
Send Window Size Number of buffers (SFTP)	Allows you to set the number of buffers to improve transfer speed. The optimum values depend on your network and server setup. Changing these values may also affect how quickly you can cancel a transfer.

SFTP button	Specifies for the FTP Client to connect using SFTP (Secure FTP) protocol. SFTP supports fewer commands than the full FTP protocol.
SSH Config Scheme	Specifies to save Secure Shell settings to the specified SSH configuration scheme and use these settings whenever you specify this SSH configuration scheme name. If you leave this blank, the current host name is used for the SSH configuration scheme name.
SSH Server address (Tunnel)	Specifies the host running your Secure Shell server. This setting is available when FTP host is different than the Secure Shell host is enabled.
SSH User name (Tunnel)	Specifies the user name on the Secure Shell server when the user login name is different on the Secure Shell and FTP servers. This setting is available when **FTP host is different than the Secure Shell host** is enabled.
Tunnel FTP using port forwarding	Specifies to forward data from the port you specify for Local port through the SSH tunnel. With this configuration you have access to the full range of FTP commands. All communications are sent through the SSH tunnel.
Use Reflection Secure Shell	Specifies to make the connection using the Secure Shell protocol. You must select this setting before you can set other items.
Use structured listing data (SFTP)	Use this setting as a troubleshooting tool if information from your Secure Shell server is missing or is not correctly displayed in the FTP Client's server pane. When this setting is not selected (the default), the FTP Client uses the standard UNIX-style data list. When it is selected, the FTP Client uses the structured data list.

Security\SSH\Host Tunneling

Port forwarding allows you to forward TCP/IP traffic through an SSH tunnel. This allows you to use the Reflection Secure Shell Client to secure data that would otherwise be sent over an unsecured TCP/IP channel. These settings are available in the Tunneling section of the Secure Shell Settings dialog box.

Add local forwarding tunnel button	Opens the Local Port Forwarding dialog box, from which you can configure ports for sending data. Outgoing data sent to the specified local port is forwarded through the secure tunnel to the specified remote host and port.
Add remote forwarding tunnel button	Opens the Remote Forwarding dialog box, from which you can configure remote port forwarding. Incoming data sent from the specified remote port is forwarded through the secure tunnel to the specified local computer and port.

Allow gateway ports	Enables gateway ports. Remote hosts are allowed to connect to local forwarded ports. By default, Reflection Secure Shell binds local port forwardings to the loopback address (this is equivalent to using "localhost"). This prevents other remote hosts from connecting to forwarded ports. **Allow gateway ports** can be used to specify that Reflection Secure Shell should bind local port forwardings to the local ethernet address (such as an IP address, a URL, or a DNS name), thus allowing remote hosts to connect to forwarded ports.
Delete local forwarding tunnel button	Removes configurations of ports for local port forwarding.
Delete remote forwarding tunnel button	Removes configurations for remote port forwarding.
Edit local forwarding tunnel button	Opens the Local Port Forwarding dialog box, from which you can change ports for sending data.
Edit remote forwarding tunnel button	Opens the Remote Forwarding dialog box, from which you can modify configurations for remote port forwarding.
Tunnel X11 connections button	Specifies that all data sent from a remote X11 port is automatically forwarded through the secure tunnel to the correct local port.

Security\SSH\User Authentication

These settings are available in the User Authentication section of the Secure Shell Settings dialog box.

Delegate credentials	Specifies whether GSSAPI forwards your ticket granting ticket (TGT) to the host. To get to this setting, select GSSAPI in the **User Authentication** section and then select **GSSAPI** in the side menu.
Use default service principle name	This setting specifies the name used to send a request for a service ticket to the Key Distribution Center (KDC). The host name value is the name of the Secure Shell server to which you are connecting. The realm value depends on which GSSAPI provider you have selected. To get to this setting, select **GSSAPI** in the **User Authentication** section and then select **GSSAPI** in the side menu.
User authentication	Use the **User Authentication** section of the Secure Shell Settings dialog box to configure your authentication preferences.

Security\SSH\User Keys

Use the User Keys section of the Secure Shell Settings dialog box to create and manage the keys that authenticate your client session to the host. To get to these settings, select **Public Key** in the **User Authentication** section and then select **User Keys** in the side menu.

Add to key agent button	Allows you to add the selected key to the Key Agent.

Allow agent forwarding	Enables forwarding of the Key Agent connection.
Change passphrase button	Allows you to change the passphrase used to protect the selected key.
Delete key button	Deletes the selected key.
Export key button	Exports a public key or public/private key pair.
Generate key button	Opens the User Key Generation dialog box, which you can use to configure a public/private key pair for user key authentication.
Import key button	Adds a private key to the list of available keys. You can use this feature to provide easy access to keys created using other applications. Importing a key copies it to the Secure Shell folder.
Launch key agent button	Opens the Reflection Key Agent tool.
Prefer SSH key signature over certificate signature	Determines the order in which the client presents certificate signature types to the server during public key authentication. When this setting is selected (the default), the client sends the key using a standard ssh key signature first (ssh-rsa or ssh-dss). If that fails, the client tries again using a certificate signature (x509-sign-rsa or x509-sign-dss).
Upload key button	Uploads a public key to the currently specified host.
Use all keys for authenticating to the host	Specifies that the client attempts to authenticate with all the listed keys, regardless of whether or not the **Use** checkbox is selected in the list of keys.
View key button	Displays the contents of the selected key or certificate.

Permissions Manager Items: Security\TLS

These settings are available from the Reflection FTP client. To get to these settings, open an FTP client settings file and click Security or create a new settings file and on the Login Information panel, click Security. Then in the Security Properties window side menu, select SSL/TLS. Click Use SSL/TLS Security to enable these options.

Item Name	Sub-group	UI Description
Clear command channel (FTP)		Specifies for the FTP Client to send a CCC command to the host that turns off encryption for the command channel only (if the host supports this option).
Connect through NAT Server (FTP)		Specifies for the FTP Client to ignore IP addresses in FTP commands returned from the server.

Item Name	Sub-group	UI Description
Encrypt data stream (FTP)		Encrypts all communication between your computer and the FTP server when the FTP client is configured to use SSL/TLS encryption. When unselected, the FTP command channel (which is used for all FTP commands, including your user name and password) is encrypted. However, the data is not encrypted.
Encryption Strength		Specifies the desired level of encryption for SSL/TLS connections.
Implicit SSL/TLS Connection		Specifies to connect to servers that are not configured to send the STARTTLS command. To connect to servers that are configured to send this command, unselect this option.
Run in FIPS Mode		Specifies to perform all connections using security protocols and algorithms that meet FIPS 140-2 standards.
Security proxy port		Specifies the proxy server port.
Security proxy server		Specifies the proxy server name.
SSL/TLS version		Specifies which SSL or TLS version to use.
Use Security proxy		Specifies to connect through the Security Proxy.
Use SSL/TLS security		Enables SSL/TLS connections.

NOTE: The **Retrieve and validate certificate chain** setting is available on the Security/PKI group.

The User Interface

With Reflection Desktop, you can display sessions in five types of user interface modes: Ribbon, Browser, TouchUx, Classic, and Classic MDI.

To select the interface type

1 Open the Reflection Workspace Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **File** menu or the Reflection button (if using the Office 2007 Look and Feel), choose **Reflection Workspace Settings**.

User Interface Mode	Steps
Reflection Browser	On the Reflection menu, choose **Settings** and then **Reflection Workspace Settings**.
TouchUx	Tap the Gear icon and then select **Reflection Workspace Settings**.

2 Click **Configure User Interface** to open the User Interface dialog box.

3 In the **User interface mode** list, select the type of interface that you want to use.

4 To select a look and feel for the Ribbon or TouchUx interfaces, choose from the options in the **Look and Feel / Color scheme** list.

5 Close and reopen the workspace

The Ribbon

The Ribbon interface shares the look and feel of Microsoft Office. In the area between the Quick Access toolbar (the toolbar in the upper-left corner) and the document window is the Ribbon, a dynamic, collapsible device that organizes commands, buttons, and other controls on tabs for each task area. Double-click any tab in the Ribbon to hide or show the Ribbon. Or, if you prefer, you can map a keyboard shortcut to show or hide the Ribbon with a keystroke. Sessions using the default 3270 or 5250 keyboard map already have this action mapped to CTRL+F1.

The Browser

The Browser interface has a look and feel that is similar to the latest Web browsers. You can access commands from the Reflection menu or from the Quick Access Toolbar. You can also access commands by searching for them in the search box and then clicking on the search results.

TouchUx

The TouchUx interface provides the Reflection TouchUx user experience. Reflection runs on Microsoft Windows devices or other devices (Apple iPad or Android) that are accessing sessions running on a Citrix server. This mode includes an on-screen terminal keyboard that can be set as a transparent overlay or docked in a separate pane.

Classic

A Classic interface option provides an interface that is familiar to users of previous versions of Reflection. When using the Classic UI, only one document can be open in a workspace, and other features may not be available.

Classic MDI

The Classic MDI interface option is similar to the Classic option. Unlike Classic, it provides a multi-document interface that allows more than one document to be open in a workspace.

Videos

▶️ Using the Reflection Ribbon (2:48)

▶️ Using the Reflection Browser (3:11)

Create New Document Dialog Box

Getting there

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	From the Quick Access Toolbar, click the **New Document** 📄 button.
TouchUx	Tap the Folder icon and then under **File**, select 📄 **New**.

Reflection provides several templates to help you start sessions and create Web page and other documents. Terminal session documents and Web page documents open in a tab in the workspace. Printer session documents open in a separate window.

Built-in templates

Built-in templates are provided with Reflection.

3270 terminal	Select to create a mainframe terminal session.
5250 terminal	Select to create an IBM System iterminal session.
3270 printer	Select to create a mainframe printer session.
5250 printer	Select to create an IBM System i printer session.
VT terminal	Select to create a UNIX, OpenVMS, or Regis Graphics terminal session.
Web	Select to access a Web page using the default browser.

User defined

User-defined templates are created when you save a document as a template.

Compatibility

Select the set of default settings to use when creating a terminal session document. The compatibility settings include keyboard maps and themes similar to those of other emulation products. The default Reflection compatibility setting is optimized for this product.

Related Topics

- "Connect and Save your Connection Settings" on page 22
- "Stop Showing the Create New Document Dialog Box" on page 113
- "Share Sessions as Templates" on page 57
- "Open a Web Session" on page 23

Change the UI Language

By default, Reflection uses the same language as the operating system to display text within the Ribbon user interface, dialog boxes, and the workspace. You can change the language for this text if you installed additional languages with Reflection, and if your operating system supports it.

To select a different language

1 Open the Reflection Workspace Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the File menu or the Reflection button ⊕ (if using the Office 2007 Look and Feel), choose **Reflection Workspace Settings**.
Reflection Browser	On the Reflection menu, choose **Settings** and then **Reflection Workspace Settings**.
TouchUx	Tap the Gear icon and then select **Reflection Workspace Settings**.

2 Under Workspace Settings, click **Configure User Interface**.

3 In the **User interface language** list, choose the language to which you want to change.

NOTE: Changes you make to the Ribbon are specific to the language selected when changes are made; for example, if you create a custom Ribbon when Spanish is selected for the user interface, that Ribbon is available only when the user interface is viewed in Spanish.

Related Topics

- "Configure Workspace Defaults Dialog Box" on page 221

Reflection Workspace Settings Dialog Box

Getting there

- Open the Reflection Workspace Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the File menu or the Reflection button ![icon] (if using the Office 2007 Look and Feel), choose **Reflection Workspace Settings**.
Reflection Browser	On the Reflection menu, choose **Settings** and then **Reflection Workspace Settings**.
TouchUx	Tap the Gear icon and then select **Reflection Workspace Settings**.

Workspace configuration settings affect all terminal session and Web page documents opened in Reflection. These settings include security, user interface options, file locations, and other settings related to Reflection.

NOTE: These settings are applied only after the workspace is closed and reopened.

Trust Center

Specify Trusted Locations	Set up trusted locations (directories that are designated as secure sources for opening files). By default, Reflection allows you to open documents only in directories that are specified as trusted locations in the Reflection settings.
Set Up Information Privacy	Configure Information Privacy features to protect sensitive data so that it is not displayed on the screen or in productivity features, such as Screen History.
Set Up API and Macro Security	Enable the Reflection .NET API, and specify corresponding settings.

Workspace Settings

Configure Workspace Defaults	Configure the actions to perform when the Reflection workspace opens or closes and preferences for automatically saving session document files.
Configure Workspace Attributes	Configure options for logging, running remote sessions, and displaying Help. You can also specify the user data directory, in which session documents and other related files are saved.
Configure User Interface	Configure which type of user interface to use (Reflection provides four interfaces), its look and feel, and other user interface options.
Configure Centralized Management	Set up the workspace to access sessions from a centralized management server.
Configure Usage Data	Choose whether to participate in the Product Experience Improvement program.

Configure Workspace Defaults Dialog Box

Getting there

1 Open the Reflection Workspace Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the File menu or the Reflection button ⚙ (if using the Office 2007 Look and Feel), choose **Reflection Workspace Settings**.
Reflection Browser	On the Reflection menu, choose **Settings** and then **Reflection Workspace Settings**.
TouchUx	Tap the Gear icon and then select **Reflection Workspace Settings**.

2 Click **Configure Workspace Defaults**.

Configure the actions to perform when the Reflection workspace opens or closes and preferences for automatically saving session document files.

Workspace

When starting workspace	Specify whether to display the New or Open dialog box or to run an action when Reflection starts.
	NOTE: When a workspace is opened by double-clicking on a session document file, this setting is not applied. (The workspace opens without displaying a dialog box or running an action.)

Select this	To do this
Show New dialog	Display the New dialog box used to choose which type of session to configure.
Show Open dialog	Display the Open dialog box used to choose a session document file.
Show nothing	Open the workspace without displaying a dialog box.
Run Startup action	Set up an action (for example, a startup macro) that is performed when Reflection starts.

Select Action	Open the Select Action dialog box used to specify actions (available only when Run Startup Action is selected).
When closing a document	Specify what you want done with any changed settings when you close a document.

Select this	To do this

	Save document settings automatically	Save the modified version of the session document and any related files without any additional prompt. If one of the modified files is a built-in file, a copy of the built-in file is saved in your user data directory.
	Ask me to save document settings	Specify where to save the modified version of the session document and any related files at the time you choose to create it.
	Discard document settings	Discard any changes to the session document and any related files.
Show Start Page after workspace opens	Displays a gallery of recent documents.	
Exit workspace when last document closed	Automatically exit Reflection after the last document (session or Web page) in the workspace is closed.	
Clear clipboard when closing workspace	When selected, any data that may have been copied to the Clipboard is cleared when the workspace is closed.	
Hide built-in templates for new documents	When selected, only user-defined templates are available from the **Create New Document** dialog box.	
Show Document Switcher with Ctr+Tab	When selected, pressing the Ctr+Tab displays a document switcher that can be used to tab through the open documents.	
Open documents in same workspace	When sessions are opened by double-clicking on session document files, the sessions all open in the same workspace.	
Prompt for disconnect	Prompt to confirm whether to disconnect a session when a session is disconnected manually or by closing the session or the workspace.	
Save session as compound document	Save all of your session settings (for keyboard maps, security settings, customized ribbons, etc.) in a single file, called a compound session document file. Using compound files simplifies the packaging process for MSI deployments.	

Recent Documents

Maximum number of Recent Documents to show	Specify the maximum number of recently used documents to display in the Recent Documents list on the "Reflection Workspace menu" on page 897.
Clear Recent Documents List	Click to remove all documents from the list.

Related Topics

- "Configure Color Settings" on page 78
- "Change the UI Language" on page 219
- "The User Interface" on page 135
- "Manage Themes Dialog Box" on page 229

Configure Workspace Attributes Dialog Box

Getting there

1 Open the Reflection Workspace Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the File menu or the Reflection button (if using the Office 2007 Look and Feel), choose **Reflection Workspace Settings**.
Reflection Browser	On the Reflection menu, choose **Settings** and then **Reflection Workspace Settings**.
TouchUx	Tap the Gear icon and then select **Reflection Workspace Settings**.

2 Click **Configure Workspace Attributes**.

You can configure options for logging, running remote sessions, and displaying Help. You can also specify the user data directory, in which session documents and other related files are saved.

Logging

Enable event logging	Select to send error information to the Windows logging service. When event logging is enabled, this information is saved in the `Workspace.log` file in the `logs` folder under the user data directory (by default, this is `%userprofile%\Documents\Micro Focus\Reflection\logs`). If centralized management is enabled, its error information is saved in the `CentralizedManagement.log` file in the same location.
Enable HLLAPI logging	Select to enable HLLAPI logging to the specified file.

Remote Session

Optimize Citrix and WTS sessions	Select to turn off cursor blinking and disable the splash screen when running Reflection under Citrix or WTS.
	NOTE: This setting is ignored if you are not running under Citrix or WTS.

Help System

When displaying help	Specify whether to use the product Help as it appears on the Micro Focus Web site or the Help installed on your local computer.
	If the Help system you specify is not available, Reflection will use the other one.
Show Help on Ribbon	Displays the Help icon and menu on the Ribbon.

Directories

Default user data directory   Type the path for the default directory in which session and other documents are saved, or click Browse to locate it. All Open and Save As dialog boxes default to this directory (including, for example, screen history and scratch pad files).

NOTE: To reopen the file later, it must be saved in a trusted location.

Default Extra! directory   Type or browse to the default directory in which to save Extra! macros or other files, such as quickpads.

Configure User Interface Dialog Box

Getting there

1 Open the Reflection Workspace Settings dialog box.

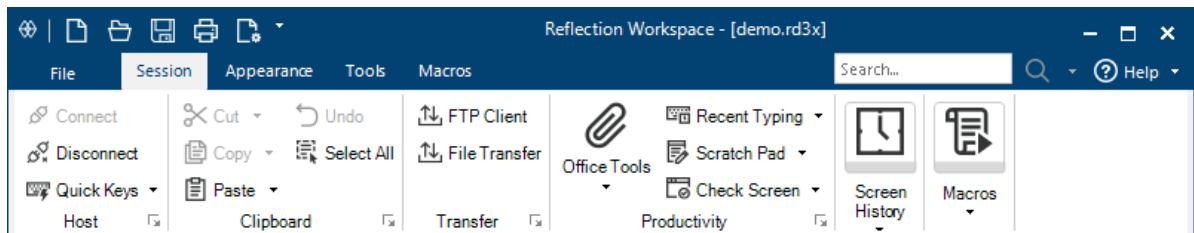The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the File menu or the Reflection button (if using the Office 2007 Look and Feel), choose **Reflection Workspace Settings**.
Reflection Browser	On the Reflection menu, choose **Settings** and then **Reflection Workspace Settings**.
TouchUx	Tap the Gear icon and then select **Reflection Workspace Settings**.

2 Click **Configure User Interface**.

You can configure which type of user interface to use (Reflection provides five interfaces), its look and feel, and other user interface options. You can also specify sounds to play when Reflection opens or closes.

UI Preferences

NOTE: If you change this setting after configuring a session, the appearance of that session may be unpredictable.

User interface mode	**Ribbon** is the default UI for Reflection. It provides a user experience similar to the most recent Microsoft Office applications, including features such as super tooltips and Ribbon galleries.
	When using the Ribbon, you can have more than one document open in the same workspace. Tabs allow you to see which documents are open, and to change between documents.
	Classic provides the familiar menu and toolbar interface. When using the Classic UI, only one document can be open in a workspace, and other features may not be available.
	NOTE: All of the Help procedures are written for the Ribbon, the Browser, or TouchUx.
	Browser provides a "minimalist" look and feel that is similar to the latest Web browsers. Multiple documents are displayed in tabs.
	TouchUx provides a touchscreen user experience. (You can run Reflection natively on Microsoft Windows 8 (or higher) devices. For iOS or Android devices, you must access Reflection through a Citrix XenApp server, with the Citrix Receiver client software installed on the device. Reflection only supports versions of Citrix software that Citrix currently supports.
	Classic MDI is similar to the Classic option. Unlike Classic, it provides a multi-document interface that allows more than one document to be open in a workspace.
Look and Feel / Color scheme	Select the base color for the application and Ribbon background. The color scheme does not affect your host screen, only the frame around it. To change the colors of the host screen, choose a different theme.
	When the Ribbon mode is selected, you can configure your workspace with two different types of "look and feel" settings that provide different ways to access the "Reflection Workspace menu" on page 897.
	With the Microsoft Office 2007 look and feel, you use the Reflection button to access the workspace menu.
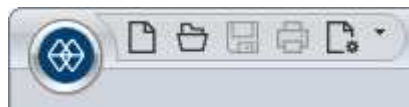
With the look and feel of more recent versions of Microsoft Office, you use the Reflection **File** menu to access the workspace menu.

When TouchUx mode is selected, you can choose an operating system look and feel (iOS, Android, or Windows). This look and feel changes only the colors and style of the display. It does not affect functionality.

For the Windows look and feel, you can select whether to open Reflection in Full Screen mode.

Arrange documents as	Documents in the workspace are displayed in tabs by default. If you are using the Reflection Ribbon, you can choose to display them in windows that can be tiled or cascaded.
Tab strip location	Specify whether to display document tabs at the top (default), bottom, left, or right.
Show Help on Ribbon	Select to display the Help button and menus on the Ribbon.
Show Close button on each tab	Clear to remove the Close button from the document tabs. Individual document tabs can still be closed using the Close button at the end of the tab strip.
Show search text input box	Select to display the Search box on the workspace.
Show Quick Access Toolbar	Select to display the Quick Access Toolbar on the Ribbon or the Browser.
Show search suggestion	Select to display search suggestions when you type in the Search box. (This applies only to Browser mode.)
Suppress Tooltips	Select to hide tooltips on the ribbon, the status bar, and the Macro Panel. (This setting does not apply to tooltips on dialog boxes or windows such as Screen History.)
Suppress Ribbon tooltip footer	Select to hide the F1 Help link that is displayed on tooltips by default.
Windows Full Screen	Select to display Reflection in full screen mode. This setting applies only to TouchUx mode.
Use alternate icons	Specify whether Reflection displays simple, "flat" toolbar icons that support a modern look and feel or the older toolbar icons used on previous versions of Reflection. When unselected (the default), the Ribbon, Browser, and TouchUx user interfaces display the modern, "flat" toolbar icons and the Classic and Classic MDI interfaces display the older icons. When selected, these default settings are switched.
User interface language	Select the language you want to use for the Reflection UI.

Sounds

Events	Select the application event with which to associate a sound.
Filename	The sound file played when the associated application event occurs.
Browse	Click to locate a sound file to associate with application events.
Play	Play the sound file associated with the selected application event.

Configure Centralized Management Dialog Box

Getting there

1 Open the Reflection Workspace Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **File** menu or the Reflection button ⚙ (if using the Office 2007 Look and Feel), choose **Reflection Workspace Settings**.
Reflection Browser	On the Reflection menu, choose **Settings** and then **Reflection Workspace Settings**.
TouchUx	Tap the Gear icon and then select **Reflection Workspace Settings**.

2 Click **Configure Centralized Management**.

If your administrator has provided you with access to a centralized management server, you can set up the workspace to access the sessions and configuration files that are managed on that server.

NOTE: After you select to use centralized management, you may need to log on when you open the Reflection Workspace, using either your domain credentials or other credentials provided by your organization.

Centralized Management

Enable centralized management	Allows the workspace to access and download session files and configuration files on a centralized management server.
Server URL	Specifies the URL of the centralized management server that manages the sessions.
Test Connection	Tests the connection for the centralized management server URL.

Options

Require authentication	When this option is selected, you are required to authenticate to a centralized management server to create or open Reflection session files, regardless of origin.
	NOTE: If this setting is selected and you are unable to authenticate to the server (for example, the network to the server is down), you will not be able to open session files and connect to host systems.
	When this option is unselected, you are not required to authenticate to the centralized management server to create or open Reflection session files. However, if the server is configured for authentication, you will still need to authenticate to the server to download centrally managed files.
Enable certificate management	Allows the workspace to access and utilize certificates on a centralized management server.

Enable automated sign-on for mainframe sessions	After you log on to the centralized management server with this option selected, you are automatically logged on to certain mainframe applications that are configured for automated sign-on when you connect to those applications. **NOTE:** You do not need to select this option to use automated sign-on for session document files that are controlled and managed by the centralized management server. To set up and configure mainframe applications for automated sign-on, see the Automated Sign-On for Mainframe Administrator Guide in the Host Access Management and Security Server Documentation.

Configure Usage Data Dialog Box

Getting there

1 Open the Reflection Workspace Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **File** menu or the Reflection button (if using the Office 2007 Look and Feel), choose **Reflection Workspace Settings**.
Reflection Browser	On the Reflection menu, choose **Settings** and then **Reflection Workspace Settings**.
TouchUx	Tap the Gear icon and then select **Reflection Workspace Settings**.

2 Click **Configure Usage Data**.

The Product Experience Improvement program is designed to help Micro Focus improve Reflection over time. This program collects information about how people use Reflection without interrupting the users in their tasks. The information that is collected helps Micro Focus identify which Reflection features to improve.

Reflection is set to participate in this program by default. If you choose not to participate, you'll need to clear the **Enable Usage Data** option and then close and reopen the workspace.

NOTE: This setting is saved in the `Application.Settings` file. If you are deploying this setting, you will need to create a package for this custom file as shown in "Configure And Automatically Package Workspace Settings" in the Reflection Deployment Guide.

Types of information that are collected when Enable Usage Data is selected

When the **Enable Usage Data** option is selected, Reflection sends telemetry data for product errors, settings, and use of features to Micro Focus, such as:

◆ Application errors

◆ Application settings such as the types of terminals used, types of secure connection settings, and whether keyboard maps or other default configuration files are customized

- Whether features such as Auto Complete or File Transfer are used
- Which types of automation (for example, VBA) are used or edited
- The duration of workspace and terminal sessions

Types of information that are not collected

Reflection does not collect personal information, information about networks, or application data such as:

- Personally identifiable information or information that identifies your organization and users
- Scripts, passwords, and data files
- Host names, IP addresses, and other information about your network
- Data directories such as trusted locations, user data directories, and application data directories
- Application data, or any other information about your applications

Manage On-Screen Keyboard Settings

Getting there

1 On the Reflection menu, tap the Gear icon and then select ▭ **Document Settings**.

2 Under **Input Devices**, click **Manage On-Screen Keyboard**.

Use the Manage On-Screen Keyboard dialog box to set up the keyboard options for the TouchUx user interface mode:

- Under **Keyboard Options**, you can set different keyboard mode options for portrait and landscape orientations.
- **Transparent** displays the keyboard as a transparent overlay on the session window. You can set the transparency level.
- **Docked** displays the keyboard in a separate pane at the bottom of the screen. The session window pane is resized to allow for the additional pane.

You can also select whether to use the device keyboard or the built-in Reflection terminal keyboard provided for the type of session you are running.

Manage Themes Dialog Box

Getting there

1 Open a terminal session.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click .
TouchUx	Tap the Gear icon and then select **Document Settings**.

2 Under **Terminal Appearance**, click **Manage Themes**.

Theme files control the colors, shape of the cursor, and other details about the appearance of your terminal sessions. When you create a terminal session document, it includes a pointer to a default, built-in theme file. You can choose a different theme file for each session, and create custom theme files with the settings you prefer.

Select another theme file	Click to choose a different theme file from a list of existing theme files. The file must be in a trusted location.
Modify the currently selected theme file	Select to modify the theme file used by this session. Because built-in files are read-only, if the currently selected file is a built-in file, it will be saved as a custom file when you change it.
Create a new theme from an existing file	Click to create a custom theme file based on an existing theme file. To reopen the file later, it must be saved in a trusted location.

Related Topics

Select a Theme File Dialog Box

Getting there

1 Open the Document Settings dialog box.

The steps depend on your .

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click .
TouchUx	Tap the Gear icon and then select **Document Settings**.

2 Under **Terminal Appearance**, click **Manage Themes**.

3 Click **Select another theme file**.

From this dialog box, select a theme file to use with this session.

Built-In	Select this option to show the theme files distributed with Reflection.
Custom	Select this option to show the theme files that you've previously modified and saved. If the file you want doesn't appear in the list, click **Browse** to select it. **NOTE:** The file must be in a trusted location.

Modify Theme Dialog Box (3270 Terminal Sessions)

Getting there

1 Open a terminal session.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ⬚.
TouchUx	Tap the Gear icon and then select ⬚ **Document Settings**.

2 Under **Terminal Appearance**, click **Manage Themes**.

3 Click **Modify the currently selected theme file.**

Create your own custom theme by modifying and saving an existing theme.

Theme Information

This information is displayed, along with a thumbnail, in the list of themes that appears on the **Select a Theme File** dialog box.

Title	Specify a title for this theme.
Description	Describe this theme.

Sounds

Make sure any sound file you want to include is saved in a trusted location. Reflection uses the sound files installed with Windows.

Events	Select the event that will trigger a sound.
Sound	Click **Browse** to specify a sound that plays when the selected event occurs. Click **Play** to hear the sound.

Font

Font Settings

Font	Select a font from the drop-down box.
Bold	Select to apply bold formatting to the specified font.
Include variable- width fonts	Select to increase your font choices.
Unicode zero character setting	Select a different style of zero, if supported by the specified font.
Automatically adjust font size to fit window	When selected, Reflection adjusts the font to fit the session screen. To specify a particular font size, select Specify font size instead.
Specify font size	Specify the point size for fonts.

Preview

Preview box	Displays the specified font and text effects.

Cursor Style

Cursor

Shape	Specify the shape for the cursor.
Blink rate	Specify the speed at which the cursor blinks.

Graphics Cursor

Shape	Specify the shape for the graphics cursor.
Crosshair color	Specify the color of the graphics cursor crosshair.

Rule Line

Show rule lines	Select to display rule lines, which provide a visual cue to your location on the screen.
Appearance	Specify the type of rule lines: a vertical line, a horizontal line, or crosshair lines.

Text Color Mapping

Terminal color	Click Change to specify the foreground (text) and background colors for all terminal session screens.
Terminal item	Click Change to specify foreground and background colors for terminal items. You can specify different colors for different types of fields: protected (read-only) and unprotected, highlighted and normal, and alpha and numeric.

Graphics Color Mapping

Terminal graphics color	Click **Change** to specify the foreground (text) colors for all terminal graphics screens.
Background	Click **Change** to specify the background color for terminal graphics screens.

Related Topics

- "Manage Themes Dialog Box" on page 229
- "Specify Trusted Locations Dialog Box" on page 426

Modify Theme Dialog Box (5250 Terminal Sessions)

Getting there

1 Open a terminal session.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ⬚.
TouchUx	Tap the Gear icon and then select ⬚ **Document Settings**.

2 Under **Terminal Appearance**, click **Manage Themes**.

3 Click **Modify the currently selected theme file.**

Create your own custom theme by modifying and saving an existing theme.

Theme Information

This information is displayed, along with a thumbnail, in the list of themes that appears on the **Select a Theme File** dialog box.

Title	Specify a title for this theme.
Description	Describe this theme.

Sounds

Make sure any sound file you want to include is saved in a trusted location. Reflection uses the sound files installed with Windows.

Events	Select the event that will trigger a sound.
Sound	Click **Browse** to specify a sound that plays when the selected event occurs. Click **Play** to hear the sound.

Font

Font Settings

Font	Select a font from the drop-down box.
Bold	Select to apply bold formatting to the specified font.
Include variable- width fonts	Select to increase your font choices.
Unicode zero character setting	Select a different style of zero, if supported by the specified font.
Automatically adjust font size to fit window	When selected, Reflection adjusts the font to fit the session screen. To specify a particular font size, select Specify font size instead.
Specify font size	Specify the point size for fonts.

Preview

Preview box	Displays the specified font and text effects.

Cursor Style

Cursor

Shape	Specify the shape for the cursor.
Blink rate	Specify the speed at which the cursor blinks.
Restrict cursor movement	When selected, cursor movement is restricted to protected fields. Selecting this option helps users navigate within the terminal screen more efficiently.
Horizontal speed	Set the horizontal cursor speed. The number indicates the number of character spaces the cursor moves with each "Left Double" or "Right Double" key press. Increase the numeric value to increase the speed.
Vertical speed	Set the vertical cursor speed. The number indicates the number of character spaces the cursor moves with each "Up Double" or "Down Double" key press. Increase the numeric value to increase the speed.

Rule Line

Show rule lines	Select to display rule lines, which provide a visual cue to your location on the screen.
Appearance	Specify the type of rule lines: a vertical line, a horizontal line, or crosshair lines.

Text Color Mapping

Terminal color	Click **Change** to specify the foreground (text) and background colors for all terminal session screens.
Terminal item	Click **Change** to specify foreground (text) and background colors for the **Status Line**, **Field Outlines**, **Message Line**, **Error Line**, and **System Request** terminal items.

Related Topics

- "Manage Themes Dialog Box" on page 229
- "Specify Trusted Locations Dialog Box" on page 426

Modify Theme Dialog Box (VT Terminal Sessions)

Getting there

1 Open a terminal session.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ⬚.
TouchUx	Tap the Gear icon and then select ⬚ **Document Settings**.

2 Under **Terminal Appearance**, click **Manage Themes**.

3 Click **Modify the currently selected theme file.**

Create your own custom theme by modifying and saving an existing theme.

Theme Information

This information is displayed, along with a thumbnail, in the list of themes that appears on the **Select a Theme File** dialog box.

Title	Specify a title for this theme.
Description	Describe this theme.

Sounds

Make sure any sound file you want to include is saved in a trusted location. Reflection uses the sound files installed with Windows.

Events	Select the event that will trigger a sound.
Sound	Click **Browse** to specify a sound that plays when the selected event occurs. Click **Play** to hear the sound.

Font

Font Settings

Font	Select a font from the drop-down box.
Bold	Select to apply bold formatting to the specified font.
Automatically adjust font size to fit window	When selected, Reflection adjusts the font to fit the session screen. To specify a particular font size, select **Specify font size** instead.
Specify font size	Specify the point size for fonts.

Preview

Preview box	Displays the specified font and text effects.

Cursor Style

Cursor

Shape	Specify the shape for the cursor.
Enable cursor blink	Select to allow the cursor to blink.

Display Enhancements

These settings control whether display enhancements specified by the host are used by your computer.

Enable blink	Select to allow text to blink.
Enable underline	Select to allow underlined text.
Enable bold	Select to allow bold text.
Inverse video	Select to allow inverse video.
Color cursor	Select to allow changes to the color of your cursor.

Text Color Mapping

These colors are not available for all terminal types.

Terminal item	Click **Change** to specify foreground and background colors for terminal items. You can specify different colors for different types of fields, such as Normal, Blink, Bold, Underline, and Inverse.

ANSI Color Mapping

These colors are not available for all terminal types.

Terminal graphics color	Click **Change** to replace standard ANSI colors with the specified colors for all terminal session screens.

Related Topics

- "Manage Themes Dialog Box" on page 229
- "Specify Trusted Locations Dialog Box" on page 426

Manage Themes Dialog Box (6530 Sessions)

Getting there

1 Open a terminal session.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ⬚.
TouchUx	Tap the Gear icon and then select ⬚ **Document Settings**.

2 Under **Terminal Appearance**, click **Manage Themes**.

Create your own custom theme by modifying the existing theme and then saving your session.

NOTE: For information about creating and editing macros, using file transfer, logging, and other features, see the 6530 Help available on the Session ribbon Help group.

Font

This information is displayed, along with a thumbnail, in the list of themes that appears on the **Select a Theme File** dialog box.

Font	Use this field to select the font to be used. The preview window below shows an example of what the font will look like.
Automatically adjust font size to fit window	If this item is checked, the font size automatically adjusts when the size of the window changes. If unchecked, the **Specify font size** field below is available, and the font size no longer changes when the window size changes.
Use ClearType font	If checked, the font is smoothed using ClearType, making it easier to read.
Specify font size	Use this field to specify the font size when Automatically adjust font size to fit window is unchecked.

Preview

Preview	Displays the specified font and text effects.

Cursor Style

Make sure any sound file you want to include is saved in a trusted location. Reflection uses the sound files installed with Windows.

Shape	This field allows you to select either a block or line style cursor.
Enable cursor blink	If checked, the cursor will blink.
	NOTE: If you run Reflection in a Citrix environment, blinking does not work regardless of this setting.

Text Color Mapping

Terminal Color	This set of fields allows users to change the color of a specific color in the new Tandem 6530 terminal extended color escape sequences. For instance, if the host send a command to place a field with the Black color (first in the list), and the user has changed that color to something else (i.e. orange), then the field uses the new orange color instead of black.
	NOTE: In most cases this set of fields should not be changed, unless the combination of foreground and background of an extended field is hard to read.
Terminal Attribute	The NonStop 6530 protocol uses attributes to designate different fields on the screen such as underlined, blinking, or invisible. Since we now use color screens, these attributes are converted to colors as per the default map.
	NOTE: You may still display the underline attribute (see here) if you wish, and you may also enable blinking on the same dialog, but all other attributes now convert to colors. Attributes can do both - i.e. blink and have a user defined color.
	To change an attributes color, just click on the **Change** button to the right of that attribute and select **Foreground Color** or **Background Color**, and then select a new color from the box of color that appears. Both the foreground and background colors can be changed, one at a time.
OSS Mode Colors	Use this field to set the base attribute colors to use in OSS mode. Only the default (Normal attribute) is defined - all others use their meaning (i.e. Underline will be the same colors with an underline).

Border Colors

Use this section to define the border colors to use in Guardian (6530) and OSS (vt220) modes.

Cursor

Use default border color	If checked and there is a border around the emulation screen, it takes on the background color of the Normal attribute. If unchecked, the fields below are active.
Guardian Mode	Use this item to set the background color while in Guardian (6530) mode.
OSS Mode	Use this item to set the background color while in OSS (vt220) mode.

QuickPads

A QuickPad is a small window that you can load during a session. QuickPads can contain text, buttons, bitmaps, icons, and other graphic elements. You can select and apply QuickPads to your session.

You can also create and modify QuickPads using the QuickPad Designer. Using the Designer, you can create QuickPads that serve a variety of needs, such as:

 * Providing interactive training tutorials for new users
 * Creating wizards that walk through processes
 * Setting up workflows that include links to Web applications or other terminal based applications
 * Providing informational overviews that link to information on the Web or other resources

For more information, see the following:

 * "Manage QuickPads Dialog Box" on page 239
 * "The QuickPad Designer" on page 240

Manage QuickPads Dialog Box

Getting to the Manage QuickPads dialog box

1 Open the Document Settings dialog box.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click .
TouchUx	Tap the Gear icon and then select **Document Settings**.
Classic MDI	With a session open, do one of the following: * If you are using a VT session, select **View Settings** on the **Setup** menu. * If you are using another type of session, go to **Options** from the **Settings** menu.

2 In the Settings dialog box, under **User Interface**, click **Manage QuickPads**.

A QuickPad is a small window that you can load during a session. QuickPads contain buttons and other controls that can be used to access macros, host functions, commands, or other actions that are available within a terminal session. You can display one or more QuickPads in a session.

To add a QuickPad or toolbar to your session

◆ Click **Select QuickPads**, select a QuickPad file, and then click **OK**.

The QuickPad is displayed in the existing session and the session document is set to display the QuickPad in new sessions.

NOTE

◆ If the QuickPad is closed during the session, it is not displayed in new sessions. To display the QuickPad, you'll need to add it to your session.

◆ Legacy toolbars are imported as QuickPads that open in a QuickPad window docked on the top of the session window.

Options

Show ToolTips	Enable tooltips on QuickPad controls.
QuickPad Selection	Opens the QuickPads Selection dialog box which displays the list of QuickPads that are available for the session. This list includes all of the QuickPad `.rqpx` files created in Reflection. It also includes all of the QuickPad (`.eqp`) files and toolbar (`.etb`) files in the `Extra!\Schemes` directory and in the Default Extra! directory specified in the "Configure Workspace Attributes Dialog Box" on page 223 (the default path is: Documents\Micro Focus\Reflection\).
Modify QuickPads	Opens the QuickPad Selection dialog box that you can use to select a QuickPad file to edit.
Create a new QuickPad	Opens the QuickPad Designer that you can use to create new QuickPads. Using the Designer, you can add buttons and other controls to your QuickPad, arrange them as needed, and map each control to an action.

For more information, see:

"Set up QuickPads" on page 86.

▶ How To Use QuickPads in Reflection Desktop (4:07)

The QuickPad Designer

Use the QuickPad Designer to create or modify QuickPads. Using the Designer, you can create QuickPads that serve a variety of needs, such as:

◆ Providing interactive training tutorials for new users

◆ Creating wizards that walk through processes

◆ Setting up workflows that include links to Web applications or other terminal based applications

◆ Providing informational overviews that link to information on the Web or other resources

After you insert controls to the Design View, you can set properties for these controls and assign any of the actions available in the Select Action Dialog Box (page 253).

NOTE: Keep in mind that the Label control can be used as a text box to display informational content. This is useful for providing instructions or other information on your QuickPad.

For more information, see:

"Set up QuickPads" on page 86.

▶️ How To Use QuickPads in Reflection Desktop (4:07)

Workspace Settings Dialog Box

Getting there

1 Open the Reflection Workspace Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **File** menu or the Reflection button ⚙, choose **Reflection Workspace Settings**.
Reflection Browser	On the Reflection menu, choose **Settings** and then **Reflection Workspace Settings**.
TouchUx	Tap the Gear icon and then select **Reflection Workspace Settings**.

2 Click **Workspace Settings**.

You can configure actions to perform when Reflection opens or closes, set workspace attributes such as the user data directory, and select which type of interface to use.

Workspace Settings

Configure Workspace Defaults	Configure the actions to perform when the Reflection workspace opens or closes and preferences for automatically saving session document files.
Configure Workspace Attributes	Configure options for logging, running remote sessions, and displaying Help. You can also specify the user data directory, in which session documents and other related files are saved.
Configure User Interface	Configure which type of user interface to use (Reflection provides four interfaces), its look and feel, and other user interface options.
Configure Centralized Management	Set up the workspace to access sessions on a centralized management server.
Configure Usage Data	Choose whether to participate in the Product Experience Improvement program.

CommandCast Panel

Getting there

1 In Reflection Desktop, open the VT session in which you want to enter the commands and the sessions you want to send commands to.

2 Open the **CommandCast** Panel as follows:

The steps depend on your .

User Interface Mode	Steps
Ribbon	On the **Tools** tab, in the **Tools** group, click the **CommandCast Panel** button.
Classic MDI	On the toolbar, click the CommandCast button 📢 .

The **CommandCast Panel** displays a list of open VT sessions.

Use the **CommandCast Panel** to broadcast commands to more than one VT session. If you manage multiple host machines, you may often need to send the same command to more than one host and reentering the command on each host can be tedious. You can save time by using CommandCast to broadcast the commands you enter in one host to any number of other hosts that you have selected to receive the commands.

You select the sessions you want to broadcast to and from in the **CommandCast Panel**. The commands you enter and the resulting output are displayed on all the host machines you are broadcasting to.

For more about how to use CommandCast, see .
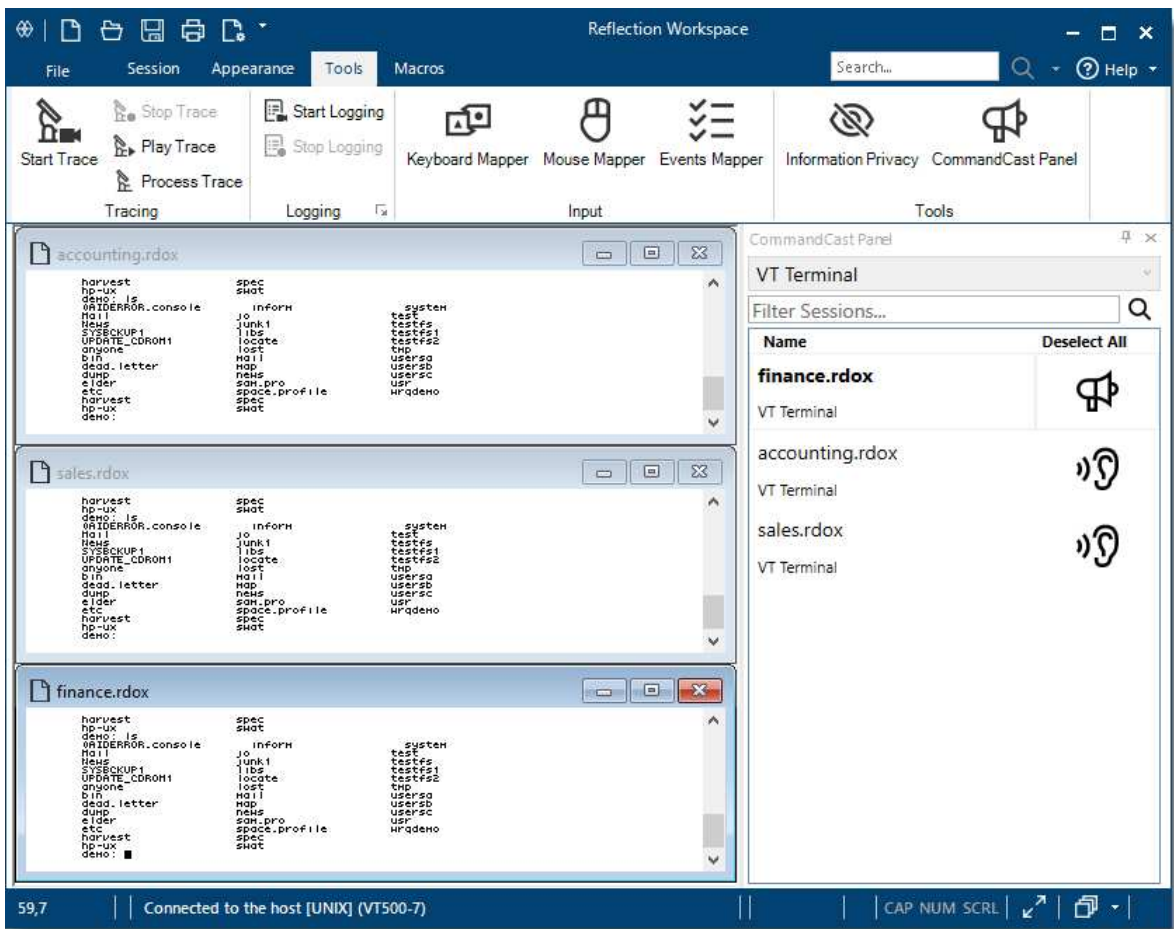
NOTE: CommandCast is supported only for VT sessions. You can use this feature for sessions you open in all user interface modes except the **Classic** user interface mode.

5 Terminal Sessions

The document for a terminal session contains configuration settings for host-specific information. It also includes pointers to other files that are used to control the appearance of the session, such as the theme file, and to files that control input and text handling, such as the keyboard map file and the Ribbon file.

Terminal sessions are preconfigured to use built-in Ribbon, theme, keyboard map, and mouse map files. If you choose, you can create custom versions of these files to modify the appearance and capabilities of each session.

CAUTION: If you specify a custom file for a session, be sure to maintain the same file name and file path (relative to the session document file) when you deploy the files. If Reflection cannot find the custom file when it starts a session, it prompts to use a built-in file.

NOTE: You must have a session open to configure it.

Access individual settings pages from specific buttons on the Ribbon. Or, click the **Document Settings** button from the **Quick Access Toolbar** to select settings pages from a list of links.

Settings pages open in a separate window that includes:

- The address path, which you can select with the click of a mouse
- Related Topics links in a pane on the left
- **Back** and **Forward** buttons, for navigation between settings pages you've visited

Session Documents and Related Files

New documents include default, built-in choices for configuration settings. These settings are saved in configuration files such as Ribbon, , keyboard map, and mouse map files. If you choose, you can create custom versions of these files to modify the appearance and capabilities of each session. If you choose a different built-in setting or create a custom setting, you must save the document to apply the new setting. Custom settings files are saved separately from the document.

Macro files are also saved as separate files external to the session document.

CAUTION: If you specify a custom file for a session, be sure to maintain the same file name and file path (relative to the session document file) when you deploy the files. If Reflection cannot find the custom file when it starts a session, it prompts to use a built-in file.

NOTE: Always save documents and templates to a trusted location — Reflection won't open documents from nontrusted locations.

You can open saved documents in any of the user interfaces modes. When using the Classic UI, only one document can be open in a workspace, and other features may not be available.

Related Topics

- "Manage Ribbon Dialog Box" on page 148
- "Keyboard Mapper" on page 273
- "Mouse Mapper" on page 277
- "Manage Themes Dialog Box" on page 229
- "Specify Trusted Locations Dialog Box" on page 426

Context Menu Editor Dialog Box

Getting there

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	Click the Appearance tab and in the **Menus** group, select **Context Menu**.
Reflection Browser	On the Reflection menu, choose **View** and then choose **Context Menu**.
TouchUx	Tap the Wrench icon and then under **View**, select **Context Menu**.
Classic IBM	On the **View** menu, choose **Context Menu**.
Classic VT	On the **Setup** menu, choose **Context Menu**.

From this dialog box, you can modify the context menu for session documents.

NOTE: Context menus in Web page documents are a function of the browser application and cannot be modified.

Select, add or remove context menu:

> This drop-down menu lists the program's default context menu and any custom context menus that have been added. Use the **Add** and **Remove** buttons to create and delete custom context menus.

Edit selected context menu:

Menu Items	Shows the items on the current context menu. An ampersand (&) before a letter indicates that you can use the ALT key with that letter to trigger the action.
Add Menu Item	Adds a new menu item below the currently selected menu item. New menu items have no defined action.
	To change the label and map an action to the new item, use the **Label** field and **Select Action** button from the **Menu Item Settings** group box.
Add Separator	Adds a new separator line below the currently selected menu item.
Delete	Removes the selected item from the context menu.
Move Up / Move Down	Moves the selected item up or down in the **Menu Items** list.

Menu Item Settings

Label	Provide a name for the menu item.
Action	The internal name for the action. To change the action, choose the **Select Action** button.
Select Action	Opens the **Select Action** dialog box, from which you can select a variety of actions, or build an action sequence.

Set up ID Management Dialog Box

Getting there

For IBM terminal sessions

1 Open an IBM3270 or IBM5250 terminal session and then open the Settings dialog box.

   The steps depend on your .

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click .
TouchUx	Tap the Gear icon and then select **Document Settings**.

2 Under **Host Connection**, click **Set Up ID Management**.

For IBM printer sessions

1 Open an IBM3270 or IBM5250 printer session.

2 From the Connection menu, choose **Session Setup**.

3 Under **Transport**, select **Use ID Management** and then click **Set up ID Management**.

ID Manager, optionally installed with your centralized management server, configures and monitors a pool of resource IDs that a client can use to establish a host session, thereby eliminating the need for administrators to create configurations for every client. Depending on the type of terminal or printer, these resource IDs may represent addresses or identifiers as required.You can use ID Manager with the IBM3270 and IBM5250 terminals and printers.To use ID Manager, you'll need access to a centralized management server with ID Manager configured.

For detailed instructions that show how to set up ID Management, see "Set Up ID Management for Reflection Desktop Sessions" in the Reflection Deployment Guide.

ID Management Settings

Reflection ID Management Server URL	The complete URL for the ID Management server. For example, `http://server.name/tidm`, where `tidm` is typically case sensitive, but `server.name` is not.
ID Selection Criteria	The parameters required by the ID Manager server to allocate an ID, such as a pool name.

Create New Web Session Document Dialog Box

Getting there

1 Open the Create New Document dialog box.

The steps depend on your .

User Interface Mode	Steps
Ribbon or Reflection Browser	From the Quick Access Toolbar, click the **New Document** button.
TouchUx	Tap the Folder icon and then under **File**, select **New**.

2 From the Create New Document dialog box, select a Web session, then click **Create**.

| URL | Type the address of the Web page you want to open. |
| | It is not necessary to type "http://" before the address. |

Related Topics

◆ "Open a Web Session" on page 23

Terminal Settings

Terminal settings consist of a variety of emulation specific options that affect the keyboard, display, and other behaviors.

◆ Configure Terminal Settings for 3270 (page 306)

◆ Configure Terminal Settings for 5250 (page 336)

◆ Configure Terminal Settings for VT (page 360)

Configuring Input and Text Handling

When you create a new session document, it is automatically configured to use the default input settings for that host. You can configure your session to use different settings, or you can customize those settings and create your own keyboard map, mouse map, and clipboard settings.

Productivity features such as Auto Complete and Auto Expand provide additional ways to customize input and text handling.

In this Section

◆ "Clear the Clipboard on Close" on page 250

◆ "Quick Keys" on page 250

◆ "Select Action Dialog Box" on page 253

◆ "Configure Clipboard Settings Dialog Box (3270 and 5250)" on page 257

◆ "Configure Clipboard Settings Dialog Box (VT)" on page 260

◆ "Configure Clipboard Settings Dialog Box (6530)" on page 261

◆ "Configure Alternate Input Device Dialog Box (6530)" on page 262

◆ "Paste Range Dialog Box" on page 263

◆ "Manage Hotspots Dialog Box" on page 265

◆ "Select a Hotspots File Dialog Box" on page 266

◆ "Modify Hotspots Dialog Box" on page 266

◆ "Hotspot Options Dialog Box" on page 267

◆ "Set Up Hotspot Display Settings Dialog Box" on page 269

◆ "Create a New Hotspots File Dialog Box" on page 271

Clear the Clipboard on Close

For security reasons, you may want to ensure that any data copied to the clipboard is cleared when you close the workspace.

To clear the clipboard automatically

1 Open Reflection Workspace Settings dialog box.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the File menu or the Reflection button ⬦ (if using the Office 2007 Look and Feel), choose **Reflection Workspace Settings**.
Reflection Browser	On the Reflection menu, choose **Settings** and then **Reflection Workspace Settings**.
TouchUx	Tap the Gear icon and then select **Reflection Workspace Settings**.

2 Click **Configure Workspace Defaults**.

3 Under **Workspace**, select **Clear clipboard when closing workspace**.

Related Topics

- "Configure Clipboard Settings Dialog Box (3270 and 5250)" on page 257
- "Copy and Paste Host Data" on page 34

Quick Keys

Use the Quick Keys gallery on the Ribbon for quick access to terminal keys for host sessions.

In this Section

- "3270 Quick Keys" on page 250
- "5250 Quick Keys" on page 251
- "VT Quick Keys" on page 252

3270 Quick Keys

In 3270 terminal sessions, the following Quick Keys are available from the Ribbon.

Program Attention Keys

PA1 - PA3	Select to send a program attention key to the host.

Program Function Keys

PF1 - PF24	Select to send a program function key to the host.

Other

Attention	Select to send an Attention key to the host.
Enter	Select to send an Enter key to the host.
Newline	Select to move the cursor to the beginning of a new line.
Erase EOF	Select to erase all characters, from the cursor to the end of the entry.
Reset	Clear the Input Inhibited indicator and reset the Insert mode.
Clear	Set buffer locations for the active partition to nulls and the Reply mode to the default, transmit the Clear Aid key to the host, and move the cursor position to the top left corner.

5250 Quick Keys

In 5250 terminal sessions, the following Quick Keys are available from the Ribbon.

Program Attention Keys

PA1 - PA3	Select to send a program attention key to the host.

Program Function Keys

PF1 - PF24	Select to send a program function key to the host.

Other

Attention	Select to send an Attention key to the host.
Enter	Select to send an Enter key to the host.
Newline	Select to move the cursor to the beginning of a new line.
Erase EOF	Select to erase all characters, from the cursor to the end of the entry.
Reset	Exit insert mode, diacritical mode, or hex mode; end help and system request functions; clear operator errors; and remove the Input Inhibited indicator and reset the Insert mode. Select **Reset** twice (consecutively) to exit Plus CR mode.
Clear	Signal the host to erase all user-entered text from the current screen.
Roll Up	Select to scroll down one page in the current host screen. This option is equivalent to Page Down.
Roll Down	Select to scroll up one page in the current host screen. This option is equivalent to Page Up.

VT Quick Keys

In VT terminal sessions, you can access a gallery of Quick Keys from the Ribbon. The specific set of keys available from the gallery depends on the terminal type your session is emulating. The standard keys for VT terminals are shown below.

Program Function Keys

PF1 - PF4	Select to send a program function key to the host.

VT Function Keys

F1 - F20	Select to send a VT function key to the host.

Edit Keys

The VT keyboard has a block of six editing keys that Reflection simulates. These keys send the following escape sequences:

Find	`<ESC>[1~`
Insert	`<ESC>[2~`
Remove	`<ESC>[3~`
Select	`<ESC>[4~`
Previous	`<ESC>[5~`
Next	`<ESC>[6~`

Reset

Clear Communications	This command:

- ◆ Cancels printing operations
- ◆ Cancels escape sequences, control sequences, and device control strings
- ◆ Turns logging off
- ◆ Clears receive and transmit buffers
- ◆ Resets XOFF (DC3) signals

For all types of connections, an XON (DC1) signal is sent to the host.

This command can often remedy communications problems when the host connection appears to be "stuck." Clear Communications does not disconnect you from the host computer.

Terminal	Also called a "soft reset," this command:
	◆ Emits a beep
	◆ Sets the main display as the active display
	◆ Cancels any pending autowrap
	◆ Sets character sets to their default values
	◆ Sets Insert/Replace mode to Replace
	◆ Unlocks the keyboard (if it was locked)
	◆ Sets the cursor keys to Normal, and the numeric keypad to Numeric
	◆ Sets the origin to Absolute
	◆ Homes the cursor
	◆ Sets Graphic Rendition and Selective Erase to Normal
	◆ Enables Text Cursor mode
	◆ Sets the top margin to 1, and the bottom to 24
	◆ Sets the UPSS to the last saved value
	◆ Initializes the communications port for serial connections to the last activated values, and clears the receive buffer
Recall Last Setup	Also called a "hard reset," this command restores the terminal settings for the active connection to their last saved settings. Settings specific to Reflection, such as file transfer settings, preferences, and printer settings, are not reset.
	In addition, this command:
	◆ Cancels a pending Wait method
	◆ Clears the display and places the cursor in the upper-left corner
	◆ Sets the select graphic rendition (SGR) function to Normal
	◆ Sets the selective erase attribute (DECSCA) to Erasable
	◆ Clears the user-defined keys (DECUDK)
	◆ Selects the default character sets: ASCII in GL and User-preferred Supplemental Set in GR
Enter	Select to send an Enter key to the host.

Select Action Dialog Box

Getting there

Because you can specify an action to complete almost any task in Reflection, there are several ways to access the Select Action dialog box:

Mouse Mapper

1 Open a session document.

2 Open the Mouse Mapper dialog box as follows:

3 Position your mouse on the image to the left and click a mouse button or mouse and key combination.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Tools** tab, click **Mouse Mapper**.
Reflection Browser	On the **Reflection** menu, choose **Tools**, and then **Mouse Mapper**.
TouchUx	Tap the Gear icon and then select **Document Settings**. Under **Input Devices**, click **Manage Mouse Map**. Then choose whether to modify the current mouse map or create a new map.

4 Click **Select Action**.

Keyboard Mapper

1 Open a session in Reflection.

2 Open the Reflection **Keyboard Mapper** dialog box as follows:

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Tools** ribbon, click **Keyboard Mapper**.
Reflection Browser	On the **Reflection** menu, choose **Tools**, and then **Keyboard Mapper**.
TouchUx	Tap the Wrench icon and then under **Tools**, select **Keyboard Mapper**.

3 Press a key or keyboard combination and then click **Select Action**.

UI Designer

1 Open a session document.

2 On the Ribbon, click the **Appearance** tab.

3 From the **Menus** group, click **UI Designer**.

4 From the **Insert Controls** pane, click the **Button** control, and then click the **Select Action** button in the **Settings** pane.

Context Menu Editor

1 Open a session document.

2 Open the Context Menu Editor as follows:

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	Click the Appearance tab and in the **Menus** group, select **Context Menu**.
Reflection Browser	On the Reflection menu, choose **View** and then choose **Context Menu**.
TouchUx	Tap the Wrench icon and then under **View**, select **Context Menu**.

3 Click **Select Action**.

Hotspots

1 Open a session document.

The steps depend on your .

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ⬛.
TouchUx	Tap the Gear icon and then select ⬛ **Document Settings**.

2 Under **Terminal Appearance**, click **Manage Hotspots**.

3 Click **Modify the currently selected hotspots file**.

4 Enter or select hotspot text, and then click **Select Action**.

From this dialog box, you can assign an action or a function to a mouse button, keyboard key, hotspot, or menu item. An action can be any action you can perform within Reflection, such as sending keystrokes, running a macro, executing a menu command, navigating to a recorded host screen page, transferring a file, or printing.

Actions are divided into categories listed in the task pane on the left, and the actions or functions available for assignment to an item depends on the selected category. Some functions also require additional information, such as the keystrokes to send for a Send Key command.

The settings for **Other Action** appear by default. A description for each task-pane item follows.

Other Action

Action category	Select from the list of feature sets that include programmable actions.
Action	Select the desired programmable action.
Action parameters	Specify any additional settings required to program the action. For example, if you select the action **Launch Application**, you must specify the application name and a working directory under **Action parameters**.

Send Key

Key	Select an Action Identifier (AID) key from the list.

Send Text

Text to send to host	Enter the text you want to send when the action runs. You can do this in two ways:
Select a special character	Select the special character to send.
	NOTE: If the **Select a special character** list doesn't have the character data you want to send, you can type in the string for the character data in the **Text to send to host** field. For example, type in <ESC>. Alternatively, you can hold down the ALT key and use the numeric keypad to enter the numeric code for the data. For example, to send <ESC>, enter 027.

Launch Application

NOTE: Before you create an action that opens a file or starts an application, place the file or application in a .

Application name	Type the name of the executable file (EXE) or click **Browse** to select it.
Parameters	Type any command line parameters you want to use to start the application.
Working directory	Type the path to the folder where the application automatically searches for files.

Open URL

Use matched hotspot text for the URL	Select this check box to create a link from any text string that matches the hotspot. The link opens the specified URL. This option is only available when mapping a hotspot to an action.
URL	Type the desired URL.
Open in new tab	Select to open the specified URL in a new Web document in the workspace.
Open in default browser	Select to start the default Web browser at the specified URL.
Open in existing tab	Select to specify an existing Web page document.
	NOTE: The document is not available from the drop-down list unless it is already open in the workspace.

Run Reflection Workspace Macro

Select macro when action occurs	Select to choose the macro each time you run the action.
Select macro	Select to specify a VBA project that contains the macro from the menu.

Action Sequence

Sequence of actions	Create and list, in order, a series of actions to be performed sequentially. Click **Add** to specify an action, **Duplicate** to add a copy of an action, **Delete** to remove an action, and **Move up** or **Move down** to change the order of the list.
Action category	Select from the list of feature sets that include programmable actions.
Action	Select the desired programmable action.
Action parameters	Specify any additional settings required to program the action. For example, if you select the action **Launch Application**, you must specify the application name and a working directory under **Action parameters**.

Related Topics

- "Specify Trusted Locations Dialog Box" on page 426
- "Add a Keyboard Shortcut" on page 64
- "Add a Mouse Action" on page 66

Configure Clipboard Settings Dialog Box (3270 and 5250)

Getting there

1 Open a terminal session.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click .
TouchUx	Tap the Gear icon and then select **Document Settings**.

2 Under **Input Devices**, select **Configure Clipboard Settings**.

Basic Editing Actions

Cut Options

Select the way you want cut or cleared characters to be filled using the following options:

Fill cut area with spaces	Replaces the characters with an equal number of spaces.
Fill cut area with nulls	Replaces the characters with an equal number of nulls.

Copy Options

Specify the behavior of text and fields that you copy using the following options:

Automatically copy selected text	Copies selected text to the clipboard automatically.
Deselect after copy	Clears selection after it has been copied to the clipboard.
Retain selection	Maintains a selected area.When you select an area of the screen, and then navigate to a new screen, the area remains selected. This allows you to copy from the same area on different screens without having to select the area again.
Copy trailing spaces	Copies the selected field, including any trailing spaces.
Copy input fields only	Copies only from areas on the screen where input is allowed. Characters in protected fields are replaced with spaces.
Copy format options	Specifies which file formats to copy from Reflection to the clipboard. If you choose more than one format, the application to which the data is pasted automatically uses the format that best suits its needs. (For example, some versions of Microsoft Word would use the RTF format.) **NOTE:** The font color for the RTF format is copied only when the **Retain color** option is selected.
Use table format	Converts two or more spaces to tabs when data is copied. If there are two or more spaces between words in a selection, the spaces are replaced with a single tab character when you copy the data. (Most spreadsheet and word processing applications interpret tab characters as cell separators.) If there is only one space between words, it remains a space when you copy the data, unless it is followed by a numerical character (0-9, +, or .). Use **Blanks between fields** to specify the number of spaces between words that should be converted to a single tab character when **Use table format** is selected.
Data delimiters	Specifies whether the data copied from Reflection should be separated by delimiters at field boundaries or at word boundaries. This option controls formatting for spreadsheet or other cell-based information and affects only the text and BIFF formats.

Paste Options

Specify the behavior of cut or copied text using the following options:

Mask protected fields	Specifies how pasted text is mapped onto the screen:
	◆ If unselected (the default), the text is interpreted as a linear stream that can contain new lines and delimiters, and is pasted accordingly.
	◆ If selected, the text is interpreted as a host screen image and overlaid onto the current screen starting at the current cursor position. Where the current screen contains an unprotected field, the source image text is pasted; where the current screen contains a protected field, the source image text is skipped.
Wrap text to next input field	Causes text that would have been truncated at the end of a field (or the selected paste area) to be pasted to the next unprotected field instead of being truncated. (This option is available only if **Mask protected fields** is not selected).
	NOTE: In most cases, if you enable this option, you should also enable **Use field delimiters**.
	Wrap to field below wraps text to the next field below instead of the next field to the right.
	Align text to input fields aligns space separated data with fields on the screen. This allows you to copy a block of data from a Word form (or other document) into a host screen that has the same field layout as the form.
Ignore field type	Controls how text is pasted on a screen that has restricted locations. If selected (the default), Reflection skips pasting text into a restricted field if the text contains an invalid entry for that field, and pastes the remaining text into subsequent fields.
	If unselected, when Reflection attempts to paste text that contains an invalid entry for a restricted field into that field, pasting stops and the screen is locked. Any remaining text is put into the Paste Next buffer. This setting applies only to IBM 5250 sessions.
Use field delimiters	Controls how text is pasted when the screen contains protected locations. If unselected, pasting stops if the first field on a row is protected. If selected, Reflection continues to search for subsequent fields, searching first right and then down, until it finds another unprotected field. If an unprotected field is located, pasting starts in this field; if not, pasting stops. When pasting is stopped, any remaining text is put into the Paste Next buffer.
Replace tabs with	Replaces any tab characters in the pasted data with the specified character or combination of characters.
Clear to end of field after paste	Clears all of the previous data remaining in a field after pasting new data into it.
Move cursor after paste	Causes the cursor to move to the end of the pasted text. When unselected, the cursor is restored to the position it was in before the text was pasted.

Configure Clipboard Settings Dialog Box (VT)

Getting there

1 Open a terminal session.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click .
TouchUx	Tap the Gear icon and then select **Document Settings**.

2 Under **Input Devices**, select **Configure Clipboard Settings**.

Basic Editing Actions

Copy Options

Specify the behavior of copied text using the following options:

Copy Format

Line by line:	Copies text on a line by line basis. All host formatting is retained.
Retain display format	Retains formatting so that copied text is pasted in the same way as it is displayed in the terminal. When unselected, formatting is removed from copied text.
Unformatted data	Copies text as data with no formatting. Carriage returns and line feeds are not copied.
Paragraph for word processing	Copies text formatted for word processing. (Insert a space at the end of each line if required to prevent words from running together.) The selected text is treated as one or more paragraphs. A carriage return and a linefeed are inserted only before a blank line.

Copy Table Method

Copies text in a tabular format that can be opened in spreadsheets.

NOTE: The Copy Format settings do not apply to text copied using the Copy Table Method.

There are two options for setting table columns:

Detect columns (using vertical spaces)	Detects columns by analyzing the data and finding spaces that line up vertically on the page.
Replace multiple spaces or tabs:	Sets columns by replacing multiple spaces or tabs with a single tab. If there is more than one space between words, the space is changed to a single tab character. Most spreadsheets and word processor tables interpret tab characters as cell separators. A single space remains a space when you copy the data, unless it is immediately followed by a numeric character (0-9, +, -. or.).

Paste Options

Specify the behavior of pasted text using the following options:

Paste buffer size	This setting specifies the size of a paste block, which is the number of characters pasted from the clipboard to the terminal window before a pause occurs. Set the length of the pause with **Paste delay**.
Paste delay	This setting specifies how many tenths of a second Reflection waits between paste blocks when pasting data from the clipboard into display memory. Set the size of the paste block with **Paste buffer size**.

Configure Clipboard Settings Dialog Box (6530)

Getting there

1 Open a terminal session.

The steps depend on your .

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ![icon].
TouchUx	Tap the Gear icon and then select ![icon] **Document Settings**.

2 Under **Input Devices**, select **Configure Clipboard Settings**.

Selection

Line	Text selection will wrap from the end of one line to the beginning of the next.
Rectangle	Text selection does not wrap across line boundaries but instead the left and right edges of the selected area fall in the same column on every line.

Paste

Map carriage return, line feed to tab	When pasting, replace any carriage return and line feed characters with a single tab character. This is useful for pasting from a document into multiple fields on a block mode screen, since Tab moves the cursor to the next field.
Replace tabs with spaces	When checked, the Number of spaces field is available, and any tabs in the pasted data are converted into the number of spaces specified in the **Number of spaces** field.

Copy Input

Add tabs between fields	If this item is checked, when performing a Copy Input menu ribbon function, which copies only unprotected fields on a block mode screen into the clipboard, tab characters are placed between the fields. This allows you to paste the fields you copied into a spreadsheet and have each field show up in the next cell, instead of everything appearing in a single cell.
Truncate trailing spaces	If this item is checked, when performing a Copy Input menu ribbon function, which copies only unprotected fields on a block mode screen into the clipboard, any trailing spaces are removed from each field.

Configure Alternate Input Device Dialog Box (6530)

Getting there

1 Open a terminal session.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ![icon].
TouchUx	Tap the Gear icon and then select ![icon] **Document Settings**.

2 Under **Input Devices**, select **Configure Alternate Input Device**.

This dialog box is used to set up an Alternate Input Device, which is usually a bar code scanner but can be any device that sends ACSII data to a field on the 6530 screen.

Alternate Input Device Configuration

Use alternate input device	Check this box to enable the Alternate Input Device.

Communications Settings

Async port	This item specifies the serial port to be used for the Alternate Input Device connection.
Data bits	This item specifies the number of data bits in each character.
Baud rate	This item specifies the speed the serial port operates at.
Stop bits	This item specifies the number of stop bits added to each character.
Parity	This item specifies the type of parity bit added to each character.

Device Settings

Enable audible alert	This item specifies whether the bell sounds after a successful read of the Alternate Input Device (AID).
Termination character	This item specifies the terminating character that the 6530 emulation expects to see at the end of the transmission from the AID. The AID device must be configurable to send one of these characters at the end of its transmission for proper operation.
Read completion action	This item specifies the action to take after a successful AID read. Valid choices are **None**, **TAB**, **ENTER**, or any NonStop function key.

Paste Range Dialog Box

Getting there

1 Select and copy some text from a terminal session or from another application to the Clipboard.

2 Open the Paste Range Dialog Box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the Session tab, on the **Paste** drop down menu, select **Paste Range**.
Classic IBM	On the **Edit** menu, select **Paste Range**.

A paste range defines a region in which you can paste text across multiple screens. After you cut, copy, or append a selection on the Clipboard, you can set the paste range before inserting the selection within the host application. (To configure how cut and paste works, see "Configure Clipboard Settings Dialog Box (3270 and 5250)" on page 257.)

TIP: You can also use the Paste Next command to paste text across multiple screens.

You will need to modify the screen positions that define the region for the paste range. You can specify different starting and ending positions for the first screen and remaining screens.

NOTE:

The changes you make in the Paste Range dialog box are retained only while your session is open and are not saved when you close your session. If you close and reopen your session, you'll need to adjust these settings again. You cannot save these settings. If you need to define a paste range that you can reuse after you close and reopen your session, you can create a VBA macro that pastes text into a custom paste range (see the PasteRange method in the VBA Help).

Paste Range is supported for IBM 3270 and IBM 5250 terminals.

Specify the paste range with the following options.

From Row	Specifies the starting row coordinate, typically a value between 1 and the last row in the terminal window.You can also specify 0 or a negative row number. If you specify 0, Reflection pastes on the last row at the bottom of the terminal window. If you specify a negative number, Reflection pastes starting at the specified number of rows from the last row. For example, if the terminal supports 24 rows and you specify -14, Reflection starts pasting on row 10.
From Col	Specifies the starting column coordinate, typically a value between 1 and the last column in the terminal window.If you specify 0, Reflection pastes on the last column at the right edge of the terminal window. If you specify a negative number, Reflection pastes starting at the specified number of columns from the last column. For example, if the terminal supports 80 columns and you specify -76, Reflection starts pasting on row 4.
To Row	Specifies the ending row coordinate, typically a value between 1 and the last row in the terminal window. If you specify 0, Reflection pastes on the last row at the bottom of the terminal window. If you specify a negative number, Reflection ends pasting at the specified number of rows from the last row. For example, if the terminal supports 24 rows and you specify -14, Reflection starts pasting on row 10.
To Col	Specifies the ending column coordinate, typically a value between 1 and the last column in the terminal window.If you specify 0, Reflection pastes on the last column at the right edge of the terminal window. If you specify a negative number, Reflection ends pasting at the specified number of columns from the last column. For example, if the terminal supports 80 columns and you specify -3, Reflection ends pasting on column 77.
Page Down Key	Specifies the terminal key used to scroll automatically to the second and remaining screens of the paste range. During the paste range operation, when the end of the screen is encountered, the Page Down key is executed automatically, scrolling to the start of the second and remaining screens.
Wrap text to next line	Inserts text across lines instead of truncating it at the end of the current line.
Use field delimiters	Controls how text is pasted when the screen contains protected locations. If unselected, pasting stops if the first field on a row is protected. If selected, Reflection continues to search for subsequent fields, searching first right and then down, until it finds another unprotected field. If an unprotected field is located, pasting starts in this field; if not, pasting stops. When pasting is stopped, any remaining text is put into the Paste Next buffer.

Templates	These templates are examples of settings for copying and pasting selections within IBM3270 host applications, such as PROFS NOTE and XEDIT, that you can use as a starting point for your application. You cannot create a custom template. If you need to define a paste range that you can reuse after you close and reopen your session, you can create a VBA macro that pastes text into a custom paste range (see the PasteRange method in the VBA Help).

Manage Hotspots Dialog Box

Getting there

1 Open a terminal session.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ![icon].
TouchUx	Tap the Gear icon and then select ![icon] **Document Settings**.

2 Under **Terminal Appearance**, click **Manage Hotspots**.

Hotspots files allow you to use your mouse to interact with your terminal session. When you create a terminal session document, it includes a pointer to a default, built-in hotspots file. You can choose a different hotspots file for each session, and you can create custom hotspots files with the settings you prefer.

NOTE: For more about how to set up and use hotspots, see "Enable and Define Hotspots" on page 85.

Select another hotspots file	Click to choose a different hotspots file from a list of existing hotspots files. The file must be in a trusted location.
Modify the currently selected hotspots file	Select to modify the hotspots file used by this session. Because built-in files are read-only, if the currently selected file is a built-in file, it will be saved as a custom file when you change it.
Create a new hotspots file from an existing hotspots file	Click to create a custom hotspots file based on an existing hotspots file. To reopen the file later, it must be saved in a trusted location.

Related Topics

◆ "Manage Mouse Map Dialog Box" on page 275

Select a Hotspots File Dialog Box

Getting there

1 Open the Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click .
TouchUx	Tap the Gear icon and then select **Document Settings**.

2 Under **Terminal Appearance**, click **Manage Hotspots**.

3 Click **Select another hotspots file**.

From this dialog box, select a hotspots file to use with this session.

Built-In	Select this option to show the hotspots files distributed with Reflection.
Custom	Select this option to show the hotspots files that you've previously modified and saved. If the file you want doesn't appear in the list, click **Browse** to select it.
	NOTE: The file must be in a trusted location.

Related Topics

◆ "Manage Hotspots Dialog Box" on page 265

Modify Hotspots Dialog Box

Getting there

1 Open a terminal session.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click .
TouchUx	Tap the Gear icon and then select **Document Settings**.

2 Under **Terminal Appearance**, click **Manage Hotspots**.

3 Click **Modify the currently selected hotspots file**.

From this dialog box, you can change the way the mouse works in Reflection. The session document uses the configured hotspots file until you reconfigure it.

NOTE

- Additional hotspots options are available in the **Set Up Hotspot Display Settings** dialog box.

- A mouse map provides additional ways to control the way your mouse works in a terminal session.

- For more about how to set up and use hotspots, see "Enable and Define Hotspots" on page 85.

Map Hotspot

Define and add hotspots to the hotspots file using the following options:

Hotspot text	Type a text string, up to 80 characters, to identify the hotspot. Reflection creates a hotspot wherever this text string is encountered in your host application.
Select Action	Select an action to associate with the specified hotspot text.

Hotspot Mapper

The hotspot mapper shows all defined hotspot text and their associated actions, which you can modify or delete.

The list shows the order in which hotspots are evaluated. If the same hotspot appears multiple times with different definitions, Reflection uses the definition that's evaluated first. Use the **Move Up** and **Move Down** buttons to change the order.

Modify	Opens the **Hotspot Options** dialog box, from which you can modify the characteristics of the hotspot, including the action associated with the hotspot text.
Delete	Removes the selected hotspot from the hotspot map.

Related Topics

Hotspot Options Dialog Box

Getting there

1 Open a terminal session.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click .
TouchUx	Tap the Gear icon and then select **Document Settings**.

2 Under **Terminal Appearance**, click **Manage Hotspots**.

3 Click **Modify the currently selected hotspots file**.

4 Under **Hotspot Mapper**, click **Modify**.

From this dialog box, you can change the action or other characteristics associated with a hotspot.

NOTE: For more about how to set up and use hotspots, see .

Hotspot Options

Modify the selected hotspot using the following options:

Hotspot text	Type a text string, up to 80 characters, to identify the hotspot. Reflection creates a hotspot wherever this text string is encountered in your host application.
Select Action	Select an action to associate with the specified hotspot text.
Tooltip	Type the text to display when the mouse cursor is over the hotspot.
Match case	Select to make the hotspot you are editing case sensitive.
Only valid at row	If selected, the hotspot will appear only if the text is in the specified row.
Only valid at column	If selected, the hotspot will appear only if the text is in the specified column.
Auto invoke when text appears on display	Select to cause the hotspot to be invoked as soon as it appears on the screen.
Text is preceded by a delimiter	Select to match the text only if the text is preceded by a delimiter specified under **Hotspot Delimiter**. For example, if you define the hotspot "host" and select this option, the word "unixhost" wouldn't be a hotspot.
Text is followed by a delimiter	Select to match the text only if the text is followed by a delimiter specified under **Hotspot Delimiter**. For example, if you define the hotspot "host" and select this option, the word "hostfile" wouldn't be a hotspot.
Match until a delimiter	Select to define the end of the hotspot as the delimiter(s) specified under **Hotspot Delimiter**.

Hotspot Delimiter

Space	Select to use the white space created by pressing the SPACEBAR as a hotspot delimiter.
Any of these characters	Select to use any of the listed characters as hotspot delimiters. When this option is selected, you can edit the list of delimiters.

Related Topics

- "Modify Hotspots Dialog Box" on page 266
- "Set Up Hotspot Display Settings Dialog Box" on page 269

Set Up Hotspot Display Settings Dialog Box

Getting there

1 Open a terminal session.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ![icon].
TouchUx	Tap the Gear icon and then select ![icon] **Document Settings**.

2 Under **Terminal Appearance**, click **Set Up Hotspot Display Settings**.

Hotspots are virtual buttons that appear in terminal sessions. By using hotspots, you can control your terminal session with the mouse instead of the keyboard. Typically, clicking a hotspot transmits a terminal key or command to the host, but you can also configure hotspots to open a Web page, launch a macro, or perform a variety of other actions.

From this dialog box, you can enable hotspots in your terminal session documents, or change the way you activate them.

NOTE: Additional hotspots options are available on the **Modify Hotspots** dialog box. For more about how to set up and use hotspots, see "Enable and Define Hotspots" on page 85.

Hotspot Display

Enable all defined hotspots	Select to enable hotspots in the current session document.
	When this check box is cleared, you can still define and maintain your hotspot configuration, but hotspots won't work or display on your screen.
Hotspot style	Select the way you want hotspots to appear on the screen.
	If you select **Not visible**, you can still use hotspots. The pointer changes to an arrow when it's over a hotspot, allowing you to invoke it by clicking the mouse, just as you would if it was visible.
Enable unprotected field hotspots	Select to display hotspots in unprotected fields.
	When this check box is cleared, the hotspots you have defined won't work or display in unprotected fields on your screen.
	NOTE: This setting does not apply to VT terminals.

Hotspot Activation

By default, a double-click with the left mouse button activates a hotspot in documents that you create from the Reflection Desktop and Extra! templates. A single click with the left mouse button activates a hotspot in documents that you create using legacy Reflection templates.

To change the activation method, use the following settings:

Choose the mouse button to activate Hotspots	Choose the mouse button (Left, Middle, or Right) that activates a hotspot.
	Select **Double-click** to require two clicks of the specified mouse button to activate a hotspot.
Choose key(s) to press in combination with mouse click	Select one or more keys to require a key press in combination with the specified mouse click settings to activate a hotspot.

NOTE: You can specify the same mouse action, or *mouse chord*, to activate a hotspot and to trigger another action. When the pointer is over the hotspot, the mouse action will activate the hotspot; in all other areas of the document, the mouse action will trigger the action you defined in the Mouse Mapper.

Default Hotspot Options

Match criteria	Select **Match case** to set the default for hotspots to be case sensitive.
Hotspot Delimiters	Select **Space** to use the white space created by pressing the SPACEBAR as a hotspot delimiter.
	Select **Any of these characters** to use any of the listed characters as hotspot delimiters. When this option is selected, you can edit the list of delimiters.

Related Topics

- "Modify Hotspots Dialog Box" on page 266
- "Hotspot Options Dialog Box" on page 267
- "Mouse Mapper" on page 277

Create a New Hotspots File Dialog Box

Getting there

1 Open a terminal session.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click [icon].
TouchUx	Tap the Gear icon and then select [icon] **Document Settings**.

2 Under **Terminal Appearance**, click **Manage Hotspots**.

3 Click **Create a new hotspots file from an existing hotspots file**.

You can create a new custom hotspots file that is based on a default hotspots file or another custom hotspots file.

NOTE: For more about how to set up and use hotspots, see "Enable and Define Hotspots" on page 85.

From this dialog box, select the hotspots file to use as a template for creating a new hotspots file.

Built-In	Select this option to show the hotspots files distributed with Reflection.
Custom	Select this option to show the hotspots files that you've previously modified and saved. If the file you want doesn't appear in the list, click **Browse** to select it. **NOTE:** The file must be in a trusted location.
Use the new file in the current session document	Select this option to use the file you are about to create with the current session.

Related Topics

- "Manage Hotspots Dialog Box" on page 265

Specifying a Custom Keyboard Map

A keyboard map lists host terminal keys and their definitions, as well as all defined keystrokes (shortcuts).

Related Topics

- "Select the Keyboard Map for a Session" on page 62
- "Create a Custom Keyboard Map" on page 63
- "Add a Keyboard Shortcut" on page 64
- "Delete a Keyboard Shortcut" on page 65
- "Restore the Default Keyboard Map" on page 65

Manage Keyboard Map Dialog Box

Getting there

1 Open a terminal session.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ▢.
TouchUx	Tap the Gear icon and then select ▢ **Document Settings**.

2 Under **Input Devices**, click **Manage Keyboard Map.**

Keyboard map files control the action of keys on your PC keyboard, so that they correspond to specific host keys or provide keyboard shortcuts. When you create a terminal session document, it includes a pointer to a default, built-in keyboard map file. You can choose a different keyboard map file for each session, and you can create custom keyboard map files with the settings you prefer.

Select another keyboard map file	Click to choose a different keyboard map file from a list of existing keyboard map files. The file must be in a trusted location.
Modify the currently selected keyboard map file	Select to modify the keyboard map file used by this session. Because built-in files are read-only, if the currently selected file is a built-in file, it will be saved as a custom file when you change it.
Create a new keyboard map from an existing file	Click to create a custom keyboard map file based on an existing keyboard map file. To reopen the file later, it must be saved in a trusted location.

Related Topics

- "Specify Trusted Locations Dialog Box" on page 426

Select a Keyboard Map File Dialog Box

Getting there

1 Open the Document Settings dialog box.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click .
TouchUx	Tap the Gear icon and then select **Document Settings**.

2 Under **Input Devices**, click **Manage Keyboard Map**.

3 Click **Select another keyboard map file**.

From this dialog box, select a keyboard map file to use with this session.

Built-In	Select this option to show the keyboard map files distributed with Reflection.
Custom	Select this option to show the keyboard map files that you've previously modified and saved. If the file you want doesn't appear in the list, click **Browse** to select it. **NOTE:** The file must be in a trusted location.

Related Topics

Keyboard Mapper

Getting there

1 Open a session in Reflection.

2 Open the Reflection **Keyboard Mapper** dialog box as follows:

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Tools** ribbon, click **Keyboard Mapper**.
Reflection Browser	On the **Reflection** menu, choose **Tools**, and then **Keyboard Mapper**.
TouchUx	Tap the Wrench icon and then under **Tools**, select **Keyboard Mapper**.

.

With the Keyboard Mapper, you can view and edit terminal keyboard maps, or create keyboard shortcuts.

Map Keys

Redefine keystrokes using the following options:

Press the key or key combination that you want to map	Define the combination of keys for the keystroke.
Reset	Resets the selected key combination to None.
Select Action	Select an action to associate with the specified keystroke.

Keyboard Mapper

This table shows you all of the defined keystrokes for the map, which you can modify.

Modify	Opens the **Select Action** dialog box, from which you can change the action associated with the keystroke.
Delete	Removes the selected keystroke from the keyboard map.

Create a New Keyboard Map File Dialog Box

Getting there

1 Open a terminal session.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ⬜.
TouchUx	Tap the Gear icon and then select ⬜ **Document Settings**.

2 Under **Input Devices**, click **Manage Keyboard Map.**

3 Click **Create a new keyboard map from an existing keyboard map file**.

From this dialog box, select the keyboard map file to use as a template for creating a new keyboard map file.

Built-In	Select this option to show the keyboard map files distributed with Reflection.
Custom	Select this option to show the keyboard map files that you've previously modified and saved. If the file you want doesn't appear in the list, click **Browse** to select it. **NOTE:** The file must be in a trusted location.
Use the new file in the current session document	Select this option to use the file you are about to create with the current session.

Related Topics

- "Create a Custom Keyboard Map" on page 63
- "Specify Trusted Locations Dialog Box" on page 426

Specifying a Mouse Map

A mouse map is a configuration file that shows all of the defined mouse actions and mouse/key combinations for your mouse. Even though session documents are pre-configured to use the built-in mouse map, you can configure the mouse to help you perform a variety of functions in Reflection. For example, you can add mouse actions that connect to hosts, start applications, and perform commands on the Reflection graphical interface.

After you add mouse actions in the **Mouse Mapper**, you can save the modified mouse map as a new, custom mouse map file, which you can use with other session documents.

Related Topics

- "Select the Mouse Map for a Session" on page 66
- "Add a Mouse Action" on page 66
- "Delete a Mouse Action" on page 67
- "Restore the Default Mouse Map" on page 68
- "Set Up Hotspot Display Settings Dialog Box" on page 269

Manage Mouse Map Dialog Box

Getting there

1 Open a terminal session.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ⬚.
TouchUx	Tap the Gear icon and then select ⬚ **Document Settings**.

2 Under **Input Devices**, click **Manage Mouse Map**.

Mouse map files control the way your mouse works in a terminal session. When you create a terminal session document, it includes a pointer to a default, built-in mouse map file. You can choose a different mouse map file for each session, and you can create custom mouse map files with the settings you prefer.

NOTE: Hotspots provide additional ways for you to use your mouse to interact with a terminal session.

Select another mouse map file	Click to choose a different mouse map file from a list of existing mouse map files. The file must be in a trusted location.
Modify the currently selected mouse map file	Select to modify the mouse map file used by this session. Because built-in files are read-only, if the currently selected file is a built-in file, it will be saved as a custom file when you change it.
Create a new mouse map from an existing file	Click to create a custom mouse map file based on an existing mouse map file. To reopen the file later, it must be saved in a trusted location.

Related Topics

- "Specify Trusted Locations Dialog Box" on page 426
- "Manage Hotspots Dialog Box" on page 265

Select a Mouse Map File Dialog Box

Getting there

1 Open the Document Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ⬚.
TouchUx	Tap the Gear icon and then select ⬚ **Document Settings**.

2 Under **Input Devices**, click **Manage Mouse Map**.

3 Click **Select another mouse map file**.

From this dialog box, select a mouse map file to use with this session.

Built-In	Select this option to show the mouse map files distributed with Reflection.
Custom	Select this option to show the mouse map files that you've previously modified and saved. If the file you want doesn't appear in the list, click **Browse** to select it.
	NOTE: The file must be in a trusted location.

Related Topics

Mouse Mapper

Getting there

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Tools** tab, click **Mouse Mapper**.
Reflection Browser	On the **Reflection** menu, choose **Tools**, and then **Mouse Mapper**.
TouchUx	Tap the Gear icon and then select **Document Settings**. Under **Input Devices**, click **Manage Mouse Map**. Then choose whether to modify the current mouse map or create a new map.

From this dialog box, you can change the way the mouse works in Reflection. The session document uses the configured mouse map until you reconfigure it.

Map Mouse Actions

Define and add mouse actions (or mouse/key combinations) to the mouse map using the following options:

Position your mouse pointer on the image to the left, then use the mouse and key combination you want to map.	Describes the mouse action or mouse/key combination after you perform it on the image to the left; for example, Ctrl+Left.
	Mouse actions include left/right click, wheel up/down, and click/key combinations.
Select Action	Select an action to associate with the specified mouse/key combination.
Reset	Clears the mouse action or mouse/key combination.

IMPORTANT: Automation for the **WheelDirection** mouse action is supported in only VBA and .NET API client programs.

Mouse Mapper

The mouse map shows all defined mouse actions and mouse/key combinations, which you can modify or delete.

Modify	Opens the **Select Action** dialog box, from which you can change the action associated with the mouse.
Delete	Removes the selected key combination from the mouse map.

Related Topics

+ "Set Up Hotspot Display Settings Dialog Box" on page 269

Create a New Mouse Map File Dialog Box

Getting there

1 Open a terminal session.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ![icon].
TouchUx	Tap the Gear icon and then select ![icon] **Document Settings**.

2 Under **Input Devices**, click **Manage Mouse Map**.

3 Click **Create a new mouse map from an existing mouse map file**.

From this dialog box, select the mouse map file to use as a template for creating a new mouse map file.

Built-In	Select this option to show the mouse map files distributed with Reflection.
Custom	Select this option to show the mouse map files that you've previously modified and saved. If the file you want doesn't appear in the list, click **Browse** to select it. **NOTE:** The file must be in a trusted location.
Use the new file in the current session document	Select this option to use the file you are about to create with the current session.

Related Topics

+ "Specify Trusted Locations Dialog Box" on page 426

Productivity Tools

Productivity features accelerate data entry and host navigation, maximizing user productivity, while reducing errors. Features such as Auto Complete, Auto Expand, Spell Check, Scratch Pad, Recent Typing, and Screen History enable users to save thousands of keystrokes throughout the day, freeing up time to serve customers more efficiently, and for more productive, revenue-producing activities.

Office Tools, Screen History, Recent Typing, and the Scratch Pad open task panes in the document window. To reopen the task panes when you open the workspace, save the workspace as a layout.

NOTE: VT sessions support only Office Tools integration, Scratch Pad, and the manual capture function of Screen History. Other productivity features are not available with VT sessions.

Office Tools Integration

The Office Tools feature allows you to integrate host data with Microsoft Office applications, if those applications are installed on your computer. You can create Word documents and PowerPoint presentations, send e-mail, schedule appointments, add notes and tasks, and create new contacts.

Screen History

Screen History creates recordings of IBM 3270 and 5250 host screens as you navigate to them. VT screens can be recorded using manual capture. You can view and/or verify the information from those screens, and send multiple host screens to Microsoft Word, PowerPoint, and Outlook (Email Message and Note only), if they are installed on your computer.

Recent Typing

Using the Recent Typing gallery or task pane, you can quickly view and select from a list of recently typed items, and send the selected string to the active document. This eliminates the need to manually re-enter information, saving time, and reducing errors when entering commonly-typed commands or field data.

Scratch Pad

Use the Scratch Pad to keep notes associated with a session. From the task pane you can print or save the Scratch Pad notes as .RTF or .TXT files.

Spelling

Set criteria for the spelling checker. With Spelling options, you can correct spelling automatically, or specify several ways to check spelling as you type.

NOTE: Spell check is not supported for Japanese.

Auto Complete

The Auto Complete feature recalls what you type, and automatically makes suggestions to help populate fields as it learns common commands that are repeated. By default, typing is saved with the screen location, and suggested when you type at that screen location again.

Auto Expand

Use the Auto Expand feature to add acronyms or shortcuts for long words, phrases, or complex repeat commands. The shortcut, when typed and followed by the Spacebar, automatically expands to the full word or phrase.

In this Section

Configure Office Tools Dialog Box

Getting there

1 Open a terminal session.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ⬚.
TouchUx	Tap the Gear icon and then select ⬚ **Document Settings**.

2 Under **Productivity**, click **Configure Office Tools**.

The Office Tools feature allows you to integrate host data with Microsoft Office applications, if those applications are installed on your computer. You can create Word documents and PowerPoint presentations, send e-mail, schedule appointments, add notes and tasks, and create new contacts.

Office Tools Defaults

Presentation template file	Set the default presentation template file.
Word-processing template file	Set the default word-processing template file.
	NOTE: This setting can also be accessed from the Office Tools task pane, which is opened by clicking **Office Tools** on the Ribbon.
Close Office documents when exiting the workspace	Select to close Office documents when exiting Reflection. If the documents are not saved, Office will prompt you to save them before closing.

Related Topics

- "Integrate Host Data with Office Tools" on page 69
- "Office Tools Dialog Box" on page 282

Configure Screen History Dialog Box

Getting there

1 Open the Document Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click .
TouchUx	Tap the Gear icon and then select **Document Settings**.

2 On the Settings dialog box, under **Productivity**, click **Configure Screen History**.

Screen History creates recordings of IBM 3270 and 5250 host screens as you navigate to them. VT screens can be recorded using manual capture. You can view and/or verify the information from those screens, and send multiple host screens to Microsoft Word, PowerPoint, and Outlook (Email Message and Note only), if they are installed on your computer.

NOTE: Only text areas of the host screen are included in the recorded image; host graphics images are not included.

Options

Maximum screens to capture	Set the maximum number of screens to record and keep at any one time in the current session's screen history.
Manual capture only	Select this check box to disable automatic screen history recording.
	Because VT supports manual capture only, this check box is not displayed for VT sessions.
Clear screen history when disconnected	When selected, the screen history is deleted when the session is disconnected for any reason. When cleared, the screen history is deleted when the session is closed.
	NOTE: If the screen history has been saved to a file, the screen history file is not affected.

Related Topics

- "Capture Screens Manually" on page 39

Office Tools Dialog Box

Getting there

1 Open the Document Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click .
TouchUx	Tap the Gear icon and then select **Document Settings**.

2 On the Settings dialog box, under **Productivity**, click **Configure Office Tools**.

NOTE: You can also access the Office Tools dialog box by clicking   in the Screen History task pane.

Use this dialog box, accessible from the Screen History task pane, to send multiple screens from Screen History to Microsoft Word, PowerPoint, and Outlook (Email Message and Note only). To use this feature, Microsoft Office applications must be installed on your computer.

NOTE: Only text areas of the host screen are included in the recorded image; host graphics images are not included.

Screens	Displays a thumbnail of all screens in the current screen history file.
Select All	Click to select all the screens in the current screen history file.
Select None	Click to clear selection of all the screens in the current screen history file.
Document type	Select the type of Microsoft Office document you want to create.
Insert screens	Select Text to insert the selected screens as text; or Images to insert the selected screens as a bitmap.

Related Topics

- "Integrate Host Data with Office Tools" on page 69
- "Configure Office Tools Dialog Box" on page 280

Configure Recent Typing Dialog Box

Getting there

1 Open the Document Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ⬚.
TouchUx	Tap the Gear icon and then select ⬚ **Document Settings**.

2 On the Settings dialog box, under **Productivity**, click **Configure Recent Typing**.

Using the Recent Typing gallery or task pane, you can quickly view and select from a list of recently typed items, and send the selected string to the active document. This eliminates the need to manually re-enter information, saving time, and reducing errors when entering commonly-typed commands or field data.

NOTE

- This feature is not available with VT sessions.

- Typing is not captured in hidden-text fields such as passwords.

Options

Number of words to remember	Reflection identifies and remembers new typed words when a field is exited by Tabkey, Spacebar,or other terminal-specific method.
Minimum word length (characters)	This feature defines the number of characters that Reflection considers a word. At the default setting of 3 characters, if you type something such as " US" into a field, it will not be remembered, and does not appear on the Recent Typing gallery and task pane.
Clear recent typing list when disconnected	When selected, the Recent Typing list is deleted when the session is disconnected for any reason. When cleared, the Recent Typing list is deleted when the session is closed.
	NOTE: If the Recent Typing list has been saved to a file, the recent typing file is not affected.

Related Topics

- "Enter Data with Recent Typing" on page 71
- "Configure Productivity Defaults Dialog Box" on page 288

Configure Auto Complete Dialog Box

Getting there

1 Open the Document Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ⬚.
TouchUx	Tap the Gear icon and then select ⬚ **Document Settings**.

2 On the Settings dialog box, under **Productivity**, click **Configure Auto Complete**.

The Auto Complete feature recalls what you type, and automatically makes suggestions to help populate fields as it learns common commands that are repeated. By default, typing is saved with the screen location, and suggested when you type at that screen location again.

NOTE

- This feature is not available with VT sessions.

- To use Auto Complete with uppercase only fields, clear the **Use case sensitivity for suggestions** option. Uppercase only fields are required to support alpha data on Japanese systems. They are also common on IBM System i systems for which 5250 emulation is used.

Options

Suggestions

Use case sensitivity for suggestions	Clear this check box to have Auto Complete ignore case when you are typing in a host field. To use Auto Complete with uppercase only fields, clear this option.
Make suggestions from all screen data	When selected, Auto Complete makes suggestions based on all user data that has been entered into any field used during the session. Field independent Auto Complete results in many more suggestions in many more screen locations.
Save suggestion data in session file	When selected, Auto Complete "remembers" the data entered during the current session, so that if the session is closed, and then reopened, suggestions will still be available.
Clear suggestions	Clears stored suggestions created from data entered by users. The next typed entry will begin creating a new set of data from which Auto Complete suggestions are made.
Characters typed before suggestions are made	After you type this number of characters, the suggestion pop-up appears.
Maximum number of suggestions	Select the maximum number of items you want Auto Complete to suggest for any word.
Maximum word length to offer suggestions on	Specify the longest word on which to apply Auto Complete. Longer words are ignored by this feature.

Overwrite and Insert

These options determine how Auto Complete behaves when entering a definition into a field with pre-existing data.

Wrap text into next field	If the Auto Complete suggestion pushes existing data past the end of the field, the additional data is added at the beginning of the next available field.
Erase to the end of the field after inserting Auto Complete suggestion	Select to have all other data in the field deleted after the Auto Complete suggestion is entered.
Insert mode	Select to maintain existing field data, with the Auto Complete suggestion inserted at the cursor location. If the insertion pushes existing data past the end of the field, the data is truncated.
Overwrite mode	Select to overwrite only the data that exists where the Auto Complete suggestion is being placed. Other data in the field will not be affected.

NOTE: Auto Complete does not record typing in hidden-text fields such as passwords, nor does it offer suggestions to complete typing in such fields.

Related Topics

- "Enter Data with Auto Complete" on page 73
- "Configure Productivity Defaults Dialog Box" on page 288

Configure Auto Expand Dialog Box

Getting there

1 Open the Document Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ![icon].
TouchUx	Tap the Gear icon and then select ![icon] **Document Settings**.

2 On the Settings dialog box, under **Productivity**, click **Configure Auto Expand**.

You can build a "dictionary" of "Auto Expand" on page 897 definitions for the current session.

NOTE

- This feature is not available with VT sessions.

- Expansion does not occur in hidden-text fields such as passwords.
- To use Auto Expand with uppercase only fields, clear the **Use case sensitivity when expanding** option. Uppercase only fields are required to support alpha data on Japanese systems. They are also common on IBM System i systems for which 5250 emulation is used.

Definitions

Select the row, or double-click in the fields to enable text entry.

*	Click to select the entire row. With the row selected, you can begin typing into the **Abbreviation** field, or you can delete the row with the Deletekey.
Abbreviation	Type the acronym or shortcut to enter on the host screen. The shortcut is expanded to the long word, phrase, or command entered in the **Expansion** field on the same row. Spaces are not permitted in the **Abbreviation** text box.
Expansion	Type the long word, phrase, or command to associate with the acronym or shortcut entered in the Abbreviation field on the same row.

Options

Use case sensitivity when expanding	Clear this check box to have Auto Expand ignore case when you are typing in a host field. Auto Expand abbreviations cannot be duplicated in the dictionary, regardless of case, even if this option is selected. To use Auto Expand with uppercase only fields, clear this option.
Wrap text into next field	Select to prevent expansions from being truncated if they don't fit in the current field. Characters that don't fit are entered into the next unprotected field on the host screen.

Overwrite and Insert

These options determine how Auto Expand behaves when entering a definition into a field with pre-existing data.

Erase to the end of the field after inserting Auto Expand definition	Select to have all other data in the field deleted after the Auto Expand definition is entered.
Insert mode	Select to maintain existing field data, with the Auto Expand definition inserted at the cursor location. If the insertion pushes existing data past the end of the field, the data is truncated.
Overwrite mode	Select to overwrite only the data that exists where the Auto Expand definition is being placed. Other data in the field is not affected.

Related Topics

◆ "Enter Data with Auto Expand" on page 74

◆ "Configure Productivity Defaults Dialog Box" on page 288

Configure Spell Checking Dialog Box

Getting there

1 Open the Document Settings dialog box.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ![icon].
TouchUx	Tap the Gear icon and then select ![icon] **Document Settings**.

2 On the Settings dialog box, under **Productivity**, click **Configure Spell Checking**.

From this settings page, you can customize the way Spell Check works.

NOTE

◆ This feature is not available with VT sessions.

◆ Spell check is not supported for Japanese.

Options

Check spelling as you type	Spell Check marks possible errors with wavy underlines.
Automatically correct spelling as you type	Commonly misspelled words are corrected without prompt or indication as you type. **NOTE:** This feature is available only for English.
Ignore words in UPPERCASE	If you are typing in UPPERCASE letters, Spell Check does not attempt to correct spelling.
Ignore words with numbers	If you are typing a word with a number in it, like `PN201`, Spell Check does not attempt to correct the spelling.
Correct TWo INitial capitals	If you type two consecutive uppercase letters at the beginning of a word, Spell Check changes the second uppercase letter to a lowercase letter; for example, `ENter` changes to `Enter`.
Correct accidental usage of cAPS LOCK key	If you accidentally type a word in Title Case with the CAPS LOCK key turned on, Spell Check corrects the capitalization; for example, `eNTER kEY` changes to `Enter Key`.

Custom dictionary file	Specify the path to the custom dictionary for the current session. For more information see the "Create a Custom Spell Check Dictionary" on page 76 topic.
Minimum field size to check spelling	Specify the shortest field in which to check spelling.
Maximum word length to check spelling	Specify the longest word to check for spelling. Longer words are ignored by the spell checker.
Maximum spelling suggestions to present	Specify the number of suggested spellings to offer when a misspelled word is encountered.
Main dictionary language	Select the language dictionary to use when checking spelling. This defaults to the language selected in the **Configure Workspace Settings** dialog box.

Related Topics

Configure Productivity Defaults Dialog Box

Getting there

1 Open the Document Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click .
TouchUx	Tap the Gear icon and then select **Document Settings**.

2 On the Settings dialog box, under **Productivity**, click **Configure Productivity Defaults**.

Use this settings page to enable or disable certain Productivity features for the current session.

NOTE: VT sessions support only Office Tools integration, Scratch Pad, and the manual capture function of Screen History. Other productivity features are not available with VT sessions.

Default Productivity Settings

Enable Recent Typing	Select to enable this feature.
	Using the Recent Typing gallery or task pane, you can quickly view and select from a list of recently typed items, and send the selected string to the active document. This eliminates the need to manually re-enter information, saving time, and reducing errors when entering commonly-typed commands or field data.
Enable Auto Complete	Select to enable this feature.
	The Auto Complete feature recalls what you type, and automatically makes suggestions to help populate fields as it learns common commands that are repeated. By default, typing is saved with the screen location, and suggested when you type at that screen location again.
Enable Auto Expand	Select to enable this feature.
	Use the Auto Expand feature to add acronyms or shortcuts for long words, phrases, or complex repeat commands. The shortcut, when typed and followed by the Spacebar, automatically expands to the full word or phrase.
Enable Spell Check	Select to enable this feature. Clearing this check box disables both automatic and manual spell check.
	NOTE: Spell check is not supported for Japanese.

Related Topics

IBM 3270 Sessions

This section includes detailed information on configuring your IBM 3270 terminal sessions.

Connect 3270 Sessions using the Express Logon Feature (ELF)

Use this procedure to configure a 3270 session to connect to the host using the "Express Logon Feature (ELF)" on page 898.

This procedure includes four parts:

1 Configure the host for ELF

2 Install digital certificates on the host and client

3 Configure ELF for a 3270 session

4 Record the connect macro that logs on using the ELF token values

---

NOTE: If you connect to the host using ELF through the a centralized management server you must configure End-to-End encryption from the Administrative Webstation. For more information, see the Reflection *Installation and Deployment Guide*.

To configure the Host for ELF

1. Configure the host to support SSL/TLS connections.

2. Configure ELF and note the applid value.

For instructions, see the documentation included with the IBM host.

To install digital certificates on the host and client

To make connections using ELF, all Reflection users must have both host and personal certificates installed. (If the certificates are from a trusted Certificate Authority, you only need to install personal certificates.) For more information, refer to Knowledge Base Article 7021686 (https://support.microfocus.com/kb/doc.php?id=7021686).

To configure ELF for a 3270 session

1 Create a new 3270 session document:

  1a Specify the **Host name/ IP Address**. If your configuration requires the host name to match the certificate, enter the name that exactly matches the CommonName or the SubjectAltName field specified in the host certificate.

  1b Specify the **Port** used for SSL connections by your host. This is configured by the IBM host administrator.

2 Select the **Configure additional settings** check box and click **OK**.

3 Under Host Connection, click **Configure Connection Settings**.

4 (Recommended) Under **Host Connection Options**, **When connection is terminated**, choose **Leave disconnected**.

Because you are configuring automatic logon, your user name and password are no longer necessary. This means you will be logged back in immediately after every log off if the default **Reconnect automatically** is selected. If you prefer to leave Auto Reconnect on while you're working, you can create a logoff macro that turns off this setting just prior to logging off.

5 Click **Configure > Advanced Connection Settings.**

6 Scroll down to **Security** and in the **ELF application ID** box, enter the applid value from the host. For example, the application ID (applid) for TSO is `TSO` appended with the `smfid` value (located in the `SMFPRMxx` member of `SYS1.PARMLIB`). For additional information, refer to the IBM system documentation.

7 Click **Security Settings** and in the **Security Properties** dialog box, do the following:

    7a Select **Use SSL/TLS security**.

    7b (Optional) Change the values for **Encryption strength** and **SSL/TLS version**.

8 Save your settings.

To record a connect macro that logs on using the ELF token values

1 Open the 3270 session file you just created. (You should be connected but not yet logged on.)

2 Start the macro recorder.

3 Log on using a valid user name and password. (Editing your macro will be easiest if you don't include your user name when you enter the logon command. Type the logon, press **Enter**, then type your user name.) You will edit the macro to remove specific user information and replace it with ELF token values that support logon by any authenticated user.

4 Stop the macro recorder.

5 In the **Stop Recording** dialog box, name the macro (for example "ELFLogon") and Click **OK**.

6 Open the Visual Basic Editor and then open the Recorded macro module.

7 In the macro you recorded, edit the `ibmCurrentScreen.SendKeys` statement that sends your user name. Remove your user name and replace it with the ELF token `)USR.ID(`. The edited line should look like this:

```
ibmCurrentScreen.SendKeys (")USR.ID(")
```

8 Comment out or delete the lines that use the `PasswordBox` function to set the password. Replace it with a new line that sets the password variable equal to the ELF password token `)PSS.WD(`. The modified code should look like this:

```
Rem hiddenTextEntry = ibmCurrentTerminal.Macro.PasswordBox("", "")
Rem If (hiddenTextEntry = "") Then
Rem     Err.Raise 5002, "Hidden TextEntry", <
     additional code on this line>...
Rem End If

ibmCurrentScreen.SendKeys (")PSS.WD(")
```

9 To set the macro you recorded to run after connection:

    9a Open the Settings window:

        The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	From the **Quick Access Toolbar**, click ⬚.
Classic	On the **Options** menu, select **Settings**.

9b Select **Configure Advanced Connection Settings**.

9c Under **Connection Action**, select **Run a macro or other action after the initial connection** and then click **Select Action** and select the macro you recorded.

9d Select **Run when reconnecting** and then close the Settings window.

10 Save the session file.

11 Connect using the modified session. The macro you created should automatically log in after you connect or reconnect. You should not have to enter a user name and password.

3270 Terminal Document Settings Dialog Box

Getting there

1 Open the Create New Document dialog box.

The steps depend on your .

User Interface Mode	Steps
Ribbon or Reflection Browser	From the Quick Access Toolbar, click the **New Document** 🗋 button.
TouchUx	Tap the Folder icon and then under **File**, select 🗋 **New**.

2 From the Create New Document dialog box, select a 3270 terminal session template, and then click **Create**.

Connection

Enter Host (or System) Name or IP Address	Identify the host to which you will connect. Type the host name, alias, or numeric IP address. **NOTE:** Both IPv4 addresses (in the form 127.0.0.1) and IPv6 addresses (in the form 2001:0db8:3c4d:0015:0000:0000:abcd:ef12) are accepted.
Port	Type the host port or socket number that the session should use. This field accepts any number between 0 and 66,535 (default = 23).
Device name	Specify a particular LU or pool of LUs (up to 32 characters) on the host. If no device name is entered, the server connects to any available LU at the specified port.
Use Telnet Extended	If selected, enables TN3270E protocols when supported.

Terminal

Terminal/Device type	Specify the model of the terminal or device type emulated by this session.
	You can select a value from the drop-down box, or type a value that is not listed. This allows you to specify a terminal model that is not implicitly supported but might work, such as Fujitsu.
	In most cases you should leave this setting at the default value. If you choose any other value, be sure to use a string that is acceptable to the host; otherwise, you may experience problems connecting to the host, and emulation problems after connecting to the host. Typically, these types of problems occur if the host is not configured to recognize the terminal specified.
Model ID	Specify the model of the terminal or device type emulated by this session.
	If the string specified in **Terminal/Device type** includes &M, the &M is replaced with the model number from this list when the string is sent to the host. For example, if IBM-3279-&M is specified and Model 3 is selected here, the string sent to the host is IBM-3279-3.
	Selecting an Extended model allows the host to specify a greater number of colors (seven instead of four) and a wider variety of display attributes. Any Model allows the gateway or mainframe to determine which model ID to use.
	Each model is associated with a terminal window display of a specific size (e.g., 24 rows by 80 columns). To specify a different number of rows or columns, select <Custom Model Extended>. When Model ID is set to <Custom Model Extended>, **Terminal/Device type** changes to IBM-DYNAMIC.
	The default value is Model 2 24x80 Extended.
Rows	The number of rows to use in the terminal window display. The valid range is 24 - 255.
	If the host application specifies a particular screen size, this value may be ignored.
Columns	The number of columns to use in the terminal window display. The valid range is 80 - 255.
	If the host application specifies a particular screen size, this value may be ignored.
Enable graphics	When selected, enables this session to emulate a graphics terminal.
	This allows you to run any host application that uses the IBM Graphics Data Display Manager (GDDM) library, such as SAS or ImageView.
Host code page	Select the language and associated host code page to be used by your session. If you are not sure which language and code page to use, check with your system administrator. The default is US English, code page 037.

Keyboard map	Specify the keyboard map to use with this session.
Configure additional settings	Select to open a page from which you can customize host connection, terminal configuration, and other settings for this session.
	When selected, the session does not auto-connect. This allows you to modify settings before connecting to the session.

Related Topics

Configure Connection Settings Dialog Box

Getting there

1 Open a 3270 terminal session.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ⬚.
TouchUx	Tap the Gear icon and then select ⬚ **Document Settings**.

2 Under **Host Connection**, click **Configure Connection Settings**.

From this dialog box, you can specify the settings for a TN3270 connection.

Connection

Host name/IP address	Identify the host to which you will connect. Type the host name, alias, or numeric IP address.
	NOTE: Both IPv4 addresses (in the form 127.0.0.1) and IPv6 addresses (in the form 2001:0db8:3c4d:0015:0000:0000:abcd:ef12) are accepted.
Port	Type the host port or socket number that the session should use. This field accepts any number between 0 and 66,535 (default = 23).
Device name	Specify a particular LU or pool of LUs (up to 32 characters) on the host. If no device name is entered, the server connects to any available LU at the specified port.

Host Connection Options

Use Telnet Extended	If selected, enables TN3270E protocols when supported.
Automatically connect to the host	Select to establish a host connection as soon as the associated session document is opened.
When connection is terminated	Specify options for reconnecting after any disconnection that is not initiated from Reflection.

Choose	To have Reflection...
Reconnect automatically	Attempt to reestablish the connection.
Prompt for reconnection	Prompt whether to attempt to reestablish the connection. (When No is selected, the session is left open and disconnected.)
Leave disconnected	Leave the session disconnected with the session open.
Close session automatically	Close the session.

Text Display

Terminal/Device type	Specify the model of the terminal or device type emulated by this session.
	You can select a value from the drop-down box, or type a value that is not listed. This allows you to specify a terminal model that is not implicitly supported but might work, such as Fujitsu.
	In most cases you should leave this setting at the default value. If you choose any other value, be sure to use a string that is acceptable to the host; otherwise, you may experience problems connecting to the host, and emulation problems after connecting to the host. Typically, these types of problems occur if the host is not configured to recognize the terminal specified.

Model ID	Specify the model of the terminal or device type emulated by this session.
	If the string specified in **Terminal/Device type** includes &M, the &M is replaced with the model number from this list when the string is sent to the host. For example, if IBM-3279-&M is specified and Model 3 is selected here, the string sent to the host is IBM-3279-3.
	Selecting an Extended model allows the host to specify a greater number of colors (seven instead of four) and a wider variety of display attributes. Any Model allows the gateway or mainframe to determine which model ID to use.
	Each model is associated with a terminal window display of a specific size (e.g., 24 rows by 80 columns). To specify a different number of rows or columns, select <Custom Model Extended>. When Model ID is set to <Custom Model Extended>, **Terminal/Device type** changes to IBM-DYNAMIC.
	The default value is Model 2 24x80 Extended.
Rows	The number of rows to use in the terminal window display. The valid range is 24 - 255.
	If the host application specifies a particular screen size, this value may be ignored.
Columns	The number of columns to use in the terminal window display. The valid range is 80 - 255.
	If the host application specifies a particular screen size, this value may be ignored.

Graphics Display

Enable graphics	When selected, enables this session to emulate a graphics terminal.
	This allows you to run any host application that uses the IBM Graphics Data Display Manager (GDDM) library, such as SAS or ImageView.
Model ID	When **Enable graphics** is selected, specifies the type of graphics terminal emulated by this session.

Related Topics

Set Up Backup Connection Settings Dialog Box

Getting there

1 Open a 3270 terminal session.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ⬜.
TouchUx	Tap the Gear icon and then select ⬜ **Document Settings**.

2 Under **Host Connection**, click **Set Up Backup Connection Settings**.

From this dialog box, you can specify the settings for one or more backup TN3270 connections. If your primary connection fails, these connections will be tried next, in the order they are listed.

Backup Hosts

Add a host to the Backup Host list by clicking the **Add** button. Use the **Move Up** and **Move Down** buttons to change the order in which the hosts are tried.

Enter Host (or System) Name or IP Address	Identify the host to which you will connect. Type the host name, alias, or numeric IP address. **NOTE:** Both IPv4 addresses (in the form 127.0.0.1) and IPv6 addresses (in the form 2001:0db8:3c4d:0015:0000:0000:abcd:ef12) are accepted.
Port	Type the host port or socket number that the session should use. This field accepts any number between 0 and 66,535 (default = 23).
Device name	Specify a particular LU or pool of LUs (up to 32 characters) on the host. If no device name is entered, the server connects to any available LU at the specified port.

Host Connection Options

When you enter more than one backup host, the connection options for each host are listed on a separate tab.

Use Telnet Extended	If selected, enables TN3270E protocols when supported.

Text Display

Terminal/Device type	Specify the model of the terminal or device type emulated by this session.
	You can select a value from the drop-down box, or type a value that is not listed. This allows you to specify a terminal model that is not implicitly supported but might work, such as Fujitsu.
	In most cases you should leave this setting at the default value. If you choose any other value, be sure to use a string that is acceptable to the host; otherwise, you may experience problems connecting to the host, and emulation problems after connecting to the host. Typically, these types of problems occur if the host is not configured to recognize the terminal specified.
Model ID	Specify the model of the terminal or device type emulated by this session.
	If the string specified in **Terminal/Device type** includes &M, the &M is replaced with the model number from this list when the string is sent to the host. For example, if IBM-3279-&M is specified and Model 3 is selected here, the string sent to the host is IBM-3279-3.
	Selecting an Extended model allows the host to specify a greater number of colors (seven instead of four) and a wider variety of display attributes. Any Model allows the gateway or mainframe to determine which model ID to use.
	Each model is associated with a terminal window display of a specific size (e.g., 24 rows by 80 columns). To specify a different number of rows or columns, select <Custom Model Extended>. When Model ID is set to <Custom Model Extended>, **Terminal/Device type** changes to IBM-DYNAMIC.
	The default value is Model 2 24x80 Extended.
Rows	The number of rows to use in the terminal window display. The valid range is 24 - 255.
	If the host application specifies a particular screen size, this value may be ignored.
Columns	The number of columns to use in the terminal window display. The valid range is 80 - 255.
	If the host application specifies a particular screen size, this value may be ignored.

Graphics Display

Enable graphics	When selected, enables this session to emulate a graphics terminal.
	This allows you to run any host application that uses the IBM Graphics Data Display Manager (GDDM) library, such as SAS or ImageView.
Model ID	When **Enable graphics** is selected, specifies the type of graphics terminal emulated by this session.

Security

Security Settings	Secure data communications with SOCKS or SSL/TLS.

Related Topics

- "Configure Connection Settings Dialog Box" on page 294
- "Configure Advanced Connection Settings Dialog Box" on page 299
- "Configure Terminal Settings Dialog Box" on page 306
- "Configure Terminal Attributes Dialog Box" on page 309

Configure Advanced Connection Settings Dialog Box

Getting there

1 Open a 3270 terminal session.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ▣.
TouchUx	Tap the Gear icon and then select ▣ **Document Settings**.

2 Under **Host Connection**, click **Configure Advanced Connection Settings**.

From this dialog box, you can define advanced TN3270 features.

Advanced TN3270

TN3270 Specific

Treat SYSREQ key as	Select the action that should be taken when you press the SYSREQ key. The definition of this key and its values vary by host application.
Treat ATTN key as	Select the action that should be taken when you press the ATTN key. The definition of this key and its values vary by host application.
Same model for primary and alternate screens	Select to use the same model type for both primary and alternate screen sizes. When selected, you can use a model type other than model 2 for primary screens.

TN3270 Enhanced Protocol

Enable associated printer	Select this option to associate a 3270 terminal session with a specific 3270 printer session, so that all print jobs from the selected terminal session are sent to the print device associated with the specified printer session.
Associated 3270 printer session	Select this option to specify the associated printer session by document name. When you use this option, the printer session starts automatically when the terminal session connects to the host.
Association string	Select this option to specify the associated printer session using an association string. The string must use only uppercase characters, and is limited to a maximum of 300 characters. The association string identifies the selected 3270 terminal session. Once you've entered the string here, you can select it from the TN Association list box when configuring the associated 3270 printer session. When you use this option, you must start the printer session before you can use it.

Connection Action

You can configure a session to run a macro, start an application, open a Web page, send an e-mail message, or perform a variety of other actions before or after it connects to the host.

Run a macro or other action before the initial connection	Select to run the connection action after the session file is opened but before the session initially connects to a host. (This action is performed even if the session is not configured to connect automatically.)
Select Action	Click to select an action to perform or a macro to run before you connect to the host. By default, the **Select Action** window opens at the screen for selecting a macro. If you prefer to perform a different action when your session connects, you can select other actions from the task pane.
Run a macro or other action after the initial connection	Select to run the connection action when the session initially connects to a host.
Select Action	Click to select an action to perform or a macro to run when you connect to the host.
Run when reconnecting	Select to run the connection action when the session initially connects to a host, and every time it reconnects to the host.

Security

ELF application ID	Specify the application ID to use the IBM Express Logon Feature (ELF). This feature allows you to connect and logon without entering a user ID and password.
	To enable this feature, click **Security Settings**, then select **Use SSL/TLS Security**. This feature also requires that you configure the host, install certificates (if necessary) on user computers, and create a connect macro. See "Connect 3270 Sessions using the Express Logon Feature (ELF)" on page 290.
Security Settings	Secure data communications with SOCKS or SSL/TLS.

Miscellaneous

Keep Alive

Send Keep Alive packets	Select to provide a constant check between your session and the host so that you become aware of connection problems as they occur.
	Choose one of the three types of keep-alive packets:

Choose	To cause
System	The TCP/IP stack to keep track of the host connection. This method requires less system resources than Send NOP Packets or Send Timing Mark Packets. However, most TCP/IP stacks send Keep Alive packets infrequently.
Send NOP Packets	Reflection to periodically send a No Operation (NOP) command to the host. The host is not required to respond to these commands, but the TCP/IP stack can detect if there was a problem delivering the packet.
Send Timing Mark Packets	Reflection to periodically send a Timing Mark Command to the host to determine if the connection is still active. The host should respond to these commands. If Reflection does not receive a response or there is an error sending the packet, it shuts down the connection.

Keep Alive timeout in seconds	Select the interval between the keep-alive requests. The range of values is 1 to 9999 seconds; the default value is 600 seconds.

Telnet Location

Telnet location	(Optional) Type up to 41 characters of descriptive text to provide information about your session. For example, you might include your PC's location, computer name, or IP address.
	This features uses the SEND-LOCATION option supported under Telnet connections (RFC779).
	Reflection does not initiate a WILL SEND command unless you activate the Telnet location option by typing information in this box.

HLLAPI

Options

Short name	Select a HLLAPI short name to associate with this session. This value is used by a HLLAPI application to identify a host session. Any single capital letter (A-Z) can be used as a short name.
	By default, Reflection assigns the first available letter (A if no other sessions are running) and saves that short name value when you save your session document. If you open multiple sessions that have the same HLLAPI short name value, Reflection automatically reassigns the HLLAPI short name of each newly opened session using the next available letter.
	If your HLLAPI application requires a specific short name value, specify this value, then save your session document. If you run multiple sessions, you must ensure that sessions running at the same time do not require the same HLLAPI short name.
	If you want Reflection to generate new, arbitrary short name values for each new session, save all session documents with the HLLAPI short name set to A. Reflection will always set the HLLAPI short name to A for the first session, and will reset the short name to the next available letter for each subsequent session.
Long name	Enter a HLLAPI long name to associate with this session. A HLLAPI long name identifies the host session for the convenience of the user. It is not used by the HLLAPI application. The long name can be up to eight characters long and can include letters, numbers, and other characters.
Compatibility	If you are migrating from an Extra! or legacy Reflection product, and your application uses the default HLLAPI compatibility settings, simply select Reflection or Extra! from the Compatibility drop-down list. This configures the HLLAPI support in Reflection to match the default settings found in those applications.
	If your application requires custom HLLAPI compatibility settings, select Custom from the Compatibility drop-down list. Once Custom is selected, you can enter a custom compatibility mask.
	NOTE: Because of variations in the implementation of HLLAPI in previous products, when HLLAPI applications from Extra! and from previous versions of Reflection are run against Reflection, they may not behave exactly as they did when run against the product for which they were originally written. Even when you have selected the correct compatibility setting, minor differences may be seen in the status or return code reported by a handful of functions.

Custom compatibility mask
The possible numeric values for the custom compatibility mask styles are "bit masks" that contain separate bits of information about Reflection's HLLAPI configuration. Each style is equated to a decimal and hexadecimal value. A list of the styles and values is shown in the table below.

To create a compatibility mask, add the decimal or hexadecimal values of each style and enter the sum into the Custom Compatibility Mask field. Values can be entered in either decimal or hexadecimal format; however, when using hexadecimal values, replace the 0x at the front of the value with &H. For example, to use hexadecimal value 0x5380, enter &H5380 in the Custom Compatibility Mask field.

For example, to turn on the Propagate EAB (decimal value = 1), Input Inhibited Position (decimal value = 8), and Don't Wrap at PS End (decimal value = 512), add these three numbers (1 + 8 + 512 = 521) and enter the total into the Compatibility Mask field.

Style	Decimal Value	Hex Value
Propagate EAB	1	0x0001
When this bit is on, executing a Copy Presentation Space or Copy Presentation Space to String function, with the EAB and NOXLATE session parameters, causes each extended attribute specified at the start of a field to be copied to all characters in the field that do not have the corresponding extended attribute explicitly on. When this bit is off, the attribute is not copied to such characters. This bit applies only to 3270 sessions.		
Query Host Update Protocol	2	0x0002
When this bit is on, Query Host Update functions report changes to the presentation space only if they are initiated by the host. When this bit is off, functions report changes initiated from the host or from the keyboard.		
Input Inhibited Position	4	0x0004
This bit determines the position of the "input inhibited" indicator in the string returned from Copy OIA. When it is on, the indicator appears at position 9. When it is off, the indicator appears at position 5.		
Copy PS to String Beyond End	8	0x0008
This bit determines what happens when the Copy Presentation Space to String function specifies a string that goes beyond the end of the presentation space. When it is on, no error is reported, the data from the position specified to the end of the presentation space is copied, and the remainder of the result string is set to binary zeros. When it is off, Reflection returns an error (APIPARAMETERERROR, value 2).		

Wait a Second	16	0x0010

When this bit is on, HLLAPI waits one second beyond the last host-initiated presentation space modification before attempting to return a result. When it is off, HLLAPI does not wait. This affects functions Copy OIA, Query Host Update, Copy Presentation Space to String, and Copy Presentation Space.

Modify Protected Field	32	0x0020

When this bit is on, the Copy Presentation Space to String function can be used to copy to protected fields. When it is off, such copies are disallowed.

Translate 5250 Attributes to 3270	64	0x0040

When this bit is on, attributes copied by the HLLAPI application from the 5250 presentation space are translated to 3270 attributes. When it is off, Reflection returns 5250 attribute values (with the high order 2 bits on).

Always Blank	128	0x0080

When this bit is on, data characters found in the presentation space (by Copy Presentation Space to String or Copy Presentation Space) that cannot be translated to ASCII are always translated to spaces. When it is off, the ATTRB setting is used to specify what should be done with such characters (if ATTRB is on, they are passed as their original value; if it is off, they are translated to spaces).

Transmit Modified Protected Fields	256	0x0100

This bit is relevant when HLLAPI modification of protected fields is allowed (see Modify Protected Field). When it is on, the modified protected field is not sent to the host in response to a read modified command. When it is off, the modified protected field is sent.

Don't Wrap at PS End	512	0x0200

This bit determines what happens if, on a copy from a string to the presentation space, the end of the presentation space is reached before the string is completely copied. If this bit is on, the operation terminates and returns an APITRUNCATED error. If it is off, copying continues at the beginning of the presentation space.

Error on Bad Escape	2048	0x0800

When this bit is on, undefined escape sequences passed to Send Key are reported by returning APIPARAMETERERROR. When it is off, such errors are ignored.

Terminate Send Key at AID	4096	0x1000

The default behavior for Send Key is to divide strings to be sent into segments terminated by an AID key, and then to send these segments sequentially, reporting an error only if the emulator objects (through input inhibited or busy status). When this bit is on, HLLAPI terminates the send after the first such segment, reporting an error if Error on Send Key Past AID is on. When this bit is off, HLLAPI does not report an error under such circumstances.

Error on Send Key Past AID	8192	0x2000

When this bit is on, the HLLAPI application reports an error if Send Key continues to send characters after a transmitted AID key. When it's off, the application does not report an error under such circumstances.

Return Zero Length Fields	16384	0x4000

If this bit is set, Find Field Position (31) returns APIOK and position of next field (in the position parameter) for a zero length field. Otherwise, it returns APIZEROLENFIELD and a 0 in the position parameter.

Caching Off	32768	0x8000

When set on, this bit disables the caching mechanism that increases performance. If you are having problems with your application synching with the Reflection screen, try turning on this bit. After enabling this bit, you may notice some degradation in HLLAPI performance.

Old Flashpoint	65536	0x10000

Flashpoint versions 3.1 and earlier expect consecutive CopyPS calls to include or not include attributes regardless of how attributes are set. Turning on this bit makes HLLAPI accept this behavior.

DOS ASCII Converter	131072	0x20000

This bit converts a HLLAPI character to DOS ASCII format.

Extra! OIA Values	262144	0x40000

When this bit is on, the Copy OIA returns OIA buffer values that match the Extra! values instead of the default Reflection values.

Rumba Style	297	0x0129

The Reflection HLLAPI configuration matches the default settings found in Rumba.

Extra! Style	21380	0x5384

The Reflection HLLAPI configuration matches the default settings found in Extra!.

Related Topics

- "Configure Connection Settings Dialog Box" on page 294
- "Set Up Backup Connection Settings Dialog Box" on page 296
- "Configure Terminal Settings Dialog Box" on page 306
- "Configure Terminal Attributes Dialog Box" on page 309

Select Host Code Page Dialog Box (3270)

Getting there

1. Open a 3270 terminal session.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ⬚.
TouchUx	Tap the Gear icon and then select ⬚ **Document Settings**.

2. Under **Terminal Configuration**, click **Select Host Code Page**.

Host Code Page

Language/Code page	Select the language and associated host code page to be used by your session. If you are not sure which language and code page to use, check with your system administrator. The default is US English, code page 037.
Enable Country Extended Code Page (CECP)	Select to make additional characters available in the configured **National character set**. See your host documentation for details.

Related Topics

- "Change the UI Language" on page 219
- "Editing a Host Code Page" on page 311

Configure Terminal Settings Dialog Box

Getting there

1. Open a 3270 terminal session.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ![icon].
TouchUx	Tap the Gear icon and then select ![icon] **Document Settings**.

2 Under **Terminal Configuration**, click **Configure Terminal Settings**.

From this dialog box, you can set input and other options for your 3270 terminal.

Input

Keyboard

Keyboard type	Specify which keys can be used in numeric fields.

Select	To use
Normal	Only number keys and certain symbol keys (such as + and -).
Data Entry	All keys.
Typewriter	Number keys, shifted number keys (producing symbols such as @ and #), and uppercase letters (A-Z).

Enable word wrap	When selected, text is wrapped to the next available field when entered text is too long to fit into the text entry field.
Enable type ahead	When selected, the characters that you type in the terminal window are buffered, allowing you to keep typing after you send data to the host.

The following 3270 functions are processed immediately and are not buffered, even when Enable Type Ahead is selected:

- Alt Cursor
- Cursor Select
- Next Window
- Pan Left
- Pan Right
- Reset
- Scroll up

Keyboard Error

Select the way you want keyboard errors to be handled.

No auto reset when a keyboard error occurs	Before you can resume data entry, you must press Reset to clear the error message.

Auto reset when a keyboard error occurs

The next key you press clears the error and attempts to execute the keystroke as follows:

If	This occurs
The cursor is in a valid input field and the key is a data key	The data is entered there if it is valid data for that field (for example, a numeric character in an input field that only accepts numbers).

Otherwise, the cursor is moved to the next valid input field, and if the data is valid for that field, it is entered there. |
| The cursor is in a valid input field and the key is a function key | The key operation is executed.

Otherwise, the cursor is moved to the next valid input field, and the key is ignored. |
| The current screen contains no valid input fields | An error message appears with each keystroke you press, and no keystrokes are executed. |

Auto reset without error message

You don't need to press Reset to clear a keyboard error. No error is reported and the next key you press attempts to execute the keystroke as follows:

If the cursor	This occurs
Is in a valid input field	The key is ignored. This is true for both data keys and function keys.
Is not in a valid input field and the key is a data key	The cursor is moved to the next valid input field, and if the data is valid for that field, it is entered there.
Is not in a valid input field and the key is a function key	The cursor is moved to the next valid input field, and the key is ignored.

Use this value with caution, because it prevents notification of keyboard errors.

Mouse

Mouse cursor shape	Select whether to display the mouse cursor as an arrow, an i-beam, or a rectangle.
Rectangular selection	Dragging the mouse across an area selects only the text within that area. When this option is cleared (unchecked), the selection wraps to line ends.

Miscellaneous

Support double-byte character set	Select to use Asian languages such as Japanese, Chinese, and Korean in your terminal session.

Related Topics

- "Configure Connection Settings Dialog Box" on page 294
- "Configure Advanced Connection Settings Dialog Box" on page 299
- "Set Up Backup Connection Settings Dialog Box" on page 296
- "Configure Terminal Attributes Dialog Box" on page 309

Configure Terminal Attributes Dialog Box

Getting there

1 Open a 3270 terminal session.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click .
TouchUx	Tap the Gear icon and then select **Document Settings**.

2 Under **Terminal Configuration**, click **Configure Terminal Attributes.**

Terminal Attributes

Enable host beep	When selected, beeps sent by the host are sounded.
Disable text blinking	When selected, text set to blink by the host does not blink.
Blink rate	Specifies the speed at which text set to blink by the host blinks.
Input field underlining	Specifies whether to underline fields that allow input. You can set options to never underline, allow the host to control underlining, or always underline.

Related Topics

◆

◆

◆

◆

Set Up Display Settings

Getting there

1 Open a 3270 terminal session.

2 If the user interface is not in **Classic** mode, set it to **Classic** as follows:

2a Open the Reflection Workspace Settings dialog box. The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **File** menu or the Reflection button ⊕, choose **Reflection Workspace Settings**.
Reflection Browser	On the Reflection menu, choose **Settings** and then **Reflection Workspace Settings**.
TouchUx	Tap the Gear icon and then select **Reflection Workspace Settings**.

2b Under **Workspace Settings**, select **Configure User Interface**.

2c In the **User interface mode** list, select **Classic**.

2d Close and reopen the Reflection Workspace.

3 On the **Options** menu, choose **Settings.**

4 Under **Terminal Configuration**, click **Set up Display Settings**.

NOTE: These settings are available for all 3270/5250 sessions running in "Classic" User interface mode.

Caption	Specifies the string that appears in the Reflection title bar.
	This string is also displayed on the taskbar when Reflection is running. If Reflection is running but minimized, the configured string is displayed on the taskbar. Type a predefined shortcut option, or enter up to 260 characters in the box. The predefined shortcuts and options are:

Shortcut	Option
&w	Micro Focus
&r	Product Name
&f	Session File Name

&s	Session Type
&t	Transport
&h	Host Name
&d	Date
&c	Connection Status (whether you are connected and over what transport)
&v	Assigned Device Name (relevant only for 5250 sessions that use an assigned Device Name)
&l	Assigned LU Name (relevant only for 3270 sessions that use an assigned LU Name)
&&	A single Ampersand

For example, if you set the Caption to &s - &t - &c, you should see text similar to "IBM 3270 Terminal - Telnet - hostname via Telnet" in the Reflection title bar or on the taskbar, assuming Reflection is running but not minimized. (The exact text depends on your configuration.) The default is &f - &r - &s.

Show Menu Bar

Display the menu and toolbar in **Classic** mode.

NOTE: When this option is unselected, you can display the menu by clicking the Reflection button ⊕ and then choosing **Show Menu Bar**.

Show Status Bar

Display the status bar in **Classic** mode.

Editing a Host Code Page

Using the Reflection Translation Table editors, you can edit the host code pages Reflection uses to translate ANSI to EBCDIC, and EBCDIC to ANSI. This makes it possible to use currently unsupported character sets, and to customize Reflection for unique host system environments.

NOTE

- ◆ Only users with administrator privileges can use this feature.
- ◆ This feature is not available with VT sessions.
- ◆ Host code page data is saved in the file R8ncs.dll, located in the Reflection installation folder (page 899). It is recommended that you make a backup copy of this file before making changes.

The translation table editors are located in the Reflection folder.

To edit this type of host code page	Use this editor
Standard 3270	`Edit3270.exe`
Standard 5250	`Edit5250.exe`
Double-byte 3270	`ed3270db.exe`
Double-byte 5250	`ed5250db.exe`

Separate tables are provided for display, file transfer, printer, and other uses. When you change an EBCDIC to ANSI translation table, you should make the corresponding change to the ANSI to EBCDIC translation table, so that the data interaction between Reflection and the host is consistent for both PC-to-host and host-to-PC transactions.

The character search window in the bottom right corner of the **Character Translation Table** tab provides a way to search for any character in a table. To search for a character, enter the character in the search window and press Enter. The table editor moves you to the location in the table that contains the character.

IBM 5250 Sessions

This section includes detailed information on configuring your IBM 5250 terminal sessions.

Input Modes and Special Characters

Special input modes available on a 5250 terminal include extended graphics mode, hex mode, insert mode, Plus CR mode, and text assist (word-processing) mode. Diacritical characters can be entered when the terminal is in extended graphics mode.

Extended Graphics Mode

The following special characters are available in extended graphics mode:

Blue indicates the character that is inserted if you press SHIFT with this key; purple indicates the character that is inserted if you press this key without SHIFT.

The default mapping for extended graphics mode is ALT+ LEFT SHIFT. When the session is in extended graphics mode, a + appears near the center of the 3488 status line.

If the **Preserve Entry Mode** check box in the Configure Terminal Settings dialog box is selected, ALT+ LEFT SHIFT functions as a toggle to take the session into and out of extended graphics mode. Reset (LEFT CTRL) also takes the session out of extended graphics mode.

If the **Preserve Entry Mode** check box is cleared, the session automatically exits extended graphics mode after you enter a graphics character or a diacritical character.

Hex Mode

On a 5250 terminal, hex mode is entered by pressing a terminal key. The default mapping for hex mode is ALT+ F7. When the session is in hex mode, the letter h or H appears on the 3488 status line.

Enter hex mode before entering a hexadecimal value for a character. To enter a hexadecimal value, type two characters. These characters can be 0-9 or a-f. No other input is allowed in hex mode.

When you enter the first character of your hex value, the h in the status line becomes a capital H. If **Preserve Entry Mode** is selected in the Configure Terminal Settings dialog box, pressing LEFT CTRL takes the character out of the buffer but doesn't exit hex mode. (You can use this method to retract the character you typed. To show this, the capital H becomes a small h once again.) Press LEFT CTRL again to back completely out of hex mode.

If **Preserve Entry Mode** is not selected, a single Reset (LEFT CTRL) takes you out of hex mode.

Insert Mode

The default mapping for insert mode is INSERT.

When the session is in insert mode, the insert symbol ($\wedge$) appears in the 3488 status line. In the 5250 status line, the letters IM are displayed in inverse video.

Characters you type when the terminal is in insert mode are inserted at the cursor position. As you type, existing characters at and to the right of the cursor position shift one position to the right for each character you type. There must be a null character at the right end of the insert field for each character you type in insert mode. If you attempt to insert more characters than there are nulls, χ appears in the status line and input is inhibited. Press Reset (LEFT CTRL) to remove the symbol and enable input.

Plus CR Mode

In this mode, a two-character hexadecimal value is displayed in front of each field in the terminal window. The meaning of the hexadecimal value is indicated by the code that appears in the status line.

Code	Hex Value Meaning
d	The field and display attributes for each field.
c	The extended character buffer values for each field.
a	The character attributes for each character in the terminal window.

The default mapping for Plus CR is ALT+ F12. Each time you press ALT+ F12, the code and hex values change to the next one in sequence. Press Reset (Left CTRL) twice to exit Plus CR mode.

Text Assist (Word-Processing) Mode

When using Text Assist mode, you can select the level of assistance (Basic or Intermediate) that you want displayed on your screen by pressing PF21in any of these three screens in OfficeVision:

- ◆ Send Note
- ◆ Work with Mail
- ◆ Work with Documents in Folders

The following word processing functions can be used in Text Assist mode on the IBM System i. If you use one of these functions when the session is not in word-processing mode results, the message "0027 = Key not supported by this emulation" is sent to your screen. (See your host documentation for more information on word-processing mode.)

Function	Keystroke	Description/Comment
Begin bold	CTRL+B	
Begin underline	CTRL+U	
Beginning of line	CTRL+LEFT ARROW	
Bottom of page	CTRL+DOWN ARROW	
Carriage return	RIGHT CTRL	CTRL+PLUS SIGN(+) and CTRL+MINUS SIGN(-) can also be used to enter a carriage return
Center text	CTRL+C	By default, CTRL+C copies text to the clipboard. To use it to center text in Text Assist mode, you must remap the key combination.
Delete at the cursor position	CTRL+DELETE	If you are currently viewing an attribute plane, this deletes the current value at the cursor position. If you are in the data plane, it deletes all values in all planes at the cursor position.
End attribute	CTRL+J	
End of line	CTRL+RIGHT ARROW	
Find next stop code	CTRL+N	By default, CTRL+N opens a new window. To use it to find the next stop code in Text Assist mode, you must remap the key combination.
Half index down	CTRL+H	

Function	Keystroke	Description/Comment
Half index up	CTRL+Y	
Insert symbols	CTRL+A	By default, CTRL+A is "Select All." To use it in Text Assist mode, you must remap the key combination.
Page end	CTRL+P	
Required carriage return	RIGHT CTRL	
Required space	CTRL+SPACEBAR	
Required tab	CTRL+TAB	To use this key combination in Text Assist mode, you must remap the key combination.
Stop	CTRL+S	To use this key combination in Text Assist mode, you must remap the key combination.
Tab	TAB	
Text tab advance	CTRL+T	Moves the cursor from the current position to the next defined tab stop. If there are no tab stops in the current field, tab advance moves the cursor to the first tab stop in the next field on the screen.
Top of page	CTRL+UP ARROW	
Word underline	CTRL+W	

Related Topics

- "Enter Diacritical Characters" on page 315

Enter Diacritical Characters

Diacritical characters are characters printed with special symbols above or below them.

To enter a diacritical character in a 5250 session

1 Put Reflection in extended graphics mode.

   The default keystroke for entering extended graphics mode is ALT+ LEFT SHIFT.

2 Press a key to indicate the diacritical mark you want to insert:

Key	Mark
g	\#193 Grave accent (`)
;	\#194 Acute accent (´)
t	\#196 Tilde (~)
f	\#195 Circumflex (^)
"	\#200 Diaerisis (¨)
'	\#203 Cedilla (¸)
d	\#202 Ring (°)

3 Press the letter key for the letter to combine with the diacritical mark. If you press SPACEBAR, the diacritical mark is inserted by itself. Only certain character choices can be combined with the diacritical character.

Mark	Characters
\#193 Grave accent (`)	a, e, i, o, u, or SPACEBAR
\#194 Acute accent (´)	a, e, i, o, u, or SPACEBAR
\#196 Tilde (~)	a, n, o, or SPACEBAR
\#195 Circumflex (^)	a, e, i, o, u, or SPACEBAR
\#200 Diaerisis (¨)	a, e, i, o, u, lowercase y, or SPACEBAR
\#203 Cedilla (¸)	c or SPACEBAR
\#202 Ring (°)	a

Status Lines

In this Section

3488 Status Line

The 3488 status line looks like this:

■ n ⌐ R ✗ ≫ nnn nnn d nnnn + ⚓ 混在 Ha A ⇧ A <S <C nn/nn

These codes and symbols in the 3488 status line are as follows:

Code	Meaning
■	System available. The session is connected to the host.
n	The 5250 session number (as low as 1, or as high as 16). As you connect 5250 terminal sessions, each new session is assigned the lowest available number. A session retains its number for as long as it is connected.
▯	Message waiting. If this icon appears, the host has one or more messages for this session.
R	Keyboard reserved. When this symbol is present, a HLLAPI application is reserving the keyboard. The keyboard is locked until the HLLAPI application releases it.
✗	Input inhibited. The system cannot process keyboard input. This symbol can appear because the system is processing input or because it has detected an error. If an error has occurred you may need to press the Help key (SCROLL LOCK) and the Reset key (LEFT CTRL) before you can start working with the host again.
>	Typeahead. An underline beneath this symbol indicates that data is in the buffer. The session can buffer up to 256 characters when the keyboard is locked (for example, while the host program is processing).
nnn	Keyboard errors. Specifies the number of keyboard errors that have occurred since the host connection was established. This information only appears when Reflection is displaying field attributes.
nnn	Link errors. Specifies the number of link parity errors that have occurred since the host connection was established. This information appears when Reflection is displaying field attributes.
d, c, or a	Plus CR mode.
nnnn	Error code. This four-digit code defines the terminal error that has occurred.
+	Extended graphics mode.
混在	Both single- and double-byte characters are accepted in the current field.
全角	Only double-byte characters are accepted in the current field.
英数	Only single-byte characters are accepted in the current field.
ᕦ	Diacritic mode. Indicates that 1) the session has been placed in extended graphics mode, and 2) one of the characters that puts Reflection in diacritic mode has been entered.
H or h	Hexadecimal mode.
a	Indicates that the ALTkey has been pressed.
A	Indicates that Caps Lock is on.
⋀	Indicates that Reflection is in Insert mode.
<S	Screen direction indicator (Arabic only). When this symbol appears, the host screen is displayed in right to left, top to bottom orientation.
<C	Cursor direction indicator (Arabic only). When this symbol displays, typing direction switches to right to left.

Code	Meaning
nn/nn	Cursor position. Specifies the location of the cursor in the terminal window in row/column format.

Related Topics

- "Configure Terminal Settings Dialog Box" on page 336
- "Status Lines" on page 316

5250 Status Line

The 5250 status line looks like this:

混在 <S <C nnnn 06/53 SA MW KS IM II KR <name> <device>

The codes in the 5250 status line are as follows:

Code	Meaning
混在	Both single- and double-byte characters are accepted in the current field.
全角	Only double-byte characters are accepted in the current field.
英数	Only single-byte characters are accepted in the current field.
<S	Screen direction indicator (Arabic only). When this symbol appears, the host screen is displayed in right to left, top to bottom orientation.
<C	Cursor direction indicator (Arabic only). When this symbol displays, typing direction switches to right to left.
nnnn	Error code. This four-digit code defines the terminal error that has occurred.
nn/nn	Cursor position. Specifies the location of the cursor in the terminal window in row/column format.
SA	System available. If SA appears in inverse video, the system is available; if SA appears in normal video, the system is unavailable.
MW	Message waiting. If MW appears in inverse video, the host has one or more messages for this session.
KS	Shift mode. If KS appears in inverse video, the SHIFTkey is being pressed.
IM	Insert mode. If IM appears in inverse video, the session is in Insert mode.
II	Input inhibited. If II appears in inverse video, the system cannot process keyboard input. If an error has occurred you may need to press the Help key (SCROLL LOCK) and the Reset key (LEFT CTRL) before you can start working with the host again.
KB	Typeahead. If KB appears in normal video, the typeahead option is on. If KB appears in inverse video, the typeahead option is on, and there are characters in the buffer. The session can buffer up to 256 characters when the keyboard is locked (for example, while the host program is processing).

Code	Meaning
KR	Keyboard reserved. When this symbol is present, a HLLAPI application is reserving the keyboard. The keyboard is locked until the HLLAPI application releases it.
<name>	The name of the system to which the session is connected.
<device>	The name of the virtual device the session is emulating.

Debug Status Line

The debug status line looks like this:

52 01   01.00.00.20.0099.5000   00   20.00.04.02   c0.c0.00.21   14/07   05f6   20/7

Most fields on the debug status line contain two-character hexadecimal numbers.

Related fields are separated by periods. For example, the string 01.00.00.20.0099.5000 near the beginning of the example status line shows six fields that contain information relating to host field attributes. Unrelated fields are separated by spaces.

If Reflection is in Plus CR mode and an error occurs, characters in positions 9-31 on the debug status line are replaced by magenta characters that provide information about the error condition. These characters are important to Micro Focus Technical Support.

Code	Meaning	
X	Input inhibit. If the "X" is present, the system cannot process keyboard input.	
<char>	**If this character is displayed**	**The session is in this mode**
	d, c, or a	Plus CR
	D	Data processing
	W	Word processing (text assist)
	U	Undefined
hex number	Pending read command. Identifies the datastream read command sent by the host.	
hex number	Field count. The total number of fields on the current screen.	
hex number	Field number. The number of the field under the cursor (if consecutive fields in a continued entry field are counted as multiple fields).	
hex number	Base field memory. The number of the field under the cursor (if consecutive fields in a continued entry field are counted as a single field).	
hex number	Field modification. The number of times the field under the cursor has been modified.	
hex number	Field display attribute. The host-defined display attribute for the field under the cursor.	
hex number	Field length. The number of characters in the field under the cursor.	
hex number	Field format word. The field attribute for the field under the cursor.	

Code	Meaning
\<character\>	The character sent by the host, enclosed in quotes.
hex number	Host data. The EBCDIC value for the character under the cursor.
hex number	Display data. The ANSI value of the character under the cursor.
hex number	Display format. The line type and font value for the character under the cursor.
hex number	Display attribute. The display attribute for the character as shown.
hex number	Display color. The color attribute for the character as shown.
hex number	ECB attribute. The extended character buffer attribute for the character under the cursor.
hex number	ECB color. The color specified by the extended character buffer for the character under the cursor.
hex number	ECB video. The video graphic value specified by the extended character buffer for the character under the cursor (not currently used).
hex number	Input field memory. Indicates the order in which fields were created. The first field created is field 00.
hex number	Field type memory. The first part of this value indicates the position of the character under the cursor within the field; the second part indicates whether the character under the cursor is detectable as a hotspot.
hex number	Cursor row. The row under the cursor.
hex number	Cursor column. The column under the cursor.
hex number	Cursor index. Indicates the cursor location in a single hex value. Numbering starts at the left end of the first row, moves right to the end of the first row, continues at the left of the second row, and so on.
decimal number	Cursor row/column. The row, column location of the cursor, represented in decimal.

Related Topics

- "Configure Terminal Settings Dialog Box" on page 336
- "Status Lines" on page 316

Configure a Device Name

In 5250 terminal sessions, the device name (also called the display name or workstation ID) is visible in the sign-on screen when you connect to your host.

You can configure the session to generate unique customized device names. Special characters can be included in the device name value to specify how the device name is displayed and incremented.

If you choose not to configure the device name, the IBM System i automatically assigns a device name for the session in the format QPADEV\<####\>.

To configure the device name

1 Open a 5250 terminal session.

2 Open the Document Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ⬜.
TouchUx	Tap the Gear icon and then select ⬜ **Document Settings**.

3 Under **Host Connection**, click **Configure Connection Settings**.

4 Verify that the **Generate a device name** check box is selected.

5 In the **Device name** field, enter a device name, then click OK and save your session.

The device name can be up to ten characters long, and it can include any of the following characters as part of the value:

This character	Specifies
*	An alphabetic counter used to create a unique device name. It is replaced by A, B, C and so on. If the entire alphabet is used, the generated device names continue with AA, AB, AC, and so on.
%	The session type. It is replaced by P for printer sessions; S for display sessions.
=	A numeric counter used to create a unique device name. It is replaced by 1, 2, 3, and so on.
&COMPN	The local workstation name, left-trimmed, if the generated name exceeds 10 characters.
&USERN	The local user name, left-trimmed, if the generated name exceeds 10 characters.
+	The use of right-trim instead of left-trim with &COMPN or &USERN. This character can be placed anywhere within the string.

NOTE

- You can use only one string in combination with these characters. If you use separated strings, the second string is dropped. For example, %MyDevice= is valid. However, %My=Device is not valid, and will be treated by the system as if it were &My=.
- You cannot use both &COMPN and &USERN in the same string.
- If you leave this box blank, the IBM System i creates a device to use for your session.

Examples:

- Setting Device name to %ABC= generates the device name SABC1 for a display session. If this is rejected, Reflection will try SABC2, SABC3, and so on.
- Setting Device name to %123* generates the device name S123A for the first display session, S123B for the second session, and so on.
- Setting Device name to &COMPN* generates puternameA, puternameB, puternameC for the first three sessions when the computer name is Computername.

◆ Setting Device name to %My=Device generates SMy. Because only one string literal can be used at a time, the second string literal (=Device) is ignored.

◆ Setting Device name to +&USERN* generates karlschmiA, karlschmiB, karlschmiC for the first three sessions when the computer user name is karlschmidt.

5250 Terminal Document Settings Dialog Box

Getting there

1 Open the Create New Document dialog box

The steps depend on your .

User Interface Mode	Steps
Ribbon or Reflection Browser	From the Quick Access Toolbar, click the **New Document** 🗋 button.
TouchUx	Tap the Folder icon and then under **File**, select 🗋 **New**.

2 From the Create New Document dialog box, select a 5250 terminal session template, and then click **Create**.

Connection

Enter Host (or System) Name or IP Address	Identify the host to which you will connect. Type the host name, alias, or numeric IP address. **NOTE:** Both IPv4 addresses (in the form 127.0.0.1) and IPv6 addresses (in the form 2001:0db8:3c4d:0015:0000:0000:abcd:ef12) are accepted.
Port	Type the host port or socket number that the session should use. This field accepts any number between 0 and 66,535 (default = 23). **NOTE:** For SSL sessions, the port defaults to 992.
Device name	Specify the terminal device name (also called the display name or the workstation ID) that the IBM System i should use for your session. If you leave this box blank, the IBM System i creates a device to use for your session. The device name can be up to ten characters long. You can include any of the following characters as part of the value in the **Device name** box.

Character	Usage
*	Replaced by A, B, C, and so on to create a unique device name. If the entire alphabet is used, the generated device names continue with AA, AB, AC, and so on.
%	Replaced by P for printer sessions and S for display sessions.

=	Replaced by 1,2, 3, and so on to create a unique device name.
&COMPN	Replaced by the local workstation name, left-trimmed, if the generated name exceeds 10 characters.
&USERN	Replaced by the local user name, left-trimmed, if the generated name exceeds 10 characters.
+	Specifies right-trimming instead of left-trimming. Use with &COMPN or &USERN. This character can be placed anywhere in the string.

NOTE

- ◆ You can use only one string in combination with these characters. If you use separated strings, the second string is dropped. For example, %MyDevice= is valid. However, %My=Device is not valid, and will be treated by the system as if it were &My=.

- ◆ You cannot use both &COMPN and &USERN in the same string.

- ◆ To have Reflection generate unique device names automatically based on the special characters described above, the Generate Device Names setting must be enabled. In printer sessions, this setting is off by default. To enable it, see the "Generate Device Names" on page 612 topic.

Generate device names

When selected, Reflection automatically generates device names based on the value specified in the **Device name** field.

For example, if the specified device name is %ABC=, Reflection generates the device name SABC1 for a display session. If SABC1 is already in use, Reflection tries SABC2, SABC3, and so on.

Setting the device name to %123* generates the device name S123A for the first display session, S123B for the second session, and so on.

When cleared, if the specified device name is in use, the session does not connect.

Terminal

Model ID	Specify the terminal (also known as a display station) you want to emulate.
Host code page	Select the language and associated host code page to be used by your session. If you are not sure which language and code page to use, check with your system administrator. The default is US English, code page 037.
K eyboard map	Specify the keyboard map to use with this session.
Configure additional settings	Select to open a page from which you can customize host connection, terminal configuration, and other settings for this session.
	When selected, the session does not auto-connect. This allows you to modify settings before connecting to the session.

Related Topics

-
-
-
-

Configure Connection Settings Dialog Box

Getting there

1 Open a 5250 terminal session.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click .
TouchUx	Tap the Gear icon and then select **Document Settings**.

2 Under **Host Connection**, click **Configure Connection Settings**.

From this dialog box, you can specify the settings for a TN5250 connection.

Connection

Enter Host (or System) Name or IP Address	Identify the host to which you will connect. Type the host name, alias, or numeric IP address.
	NOTE: Both IPv4 addresses (in the form 127.0.0.1) and IPv6 addresses (in the form 2001:0db8:3c4d:0015:0000:0000:abcd:ef12) are accepted.
Port	Type the host port or socket number that the session should use. This field accepts any number between 0 and 66,535 (default = 23).

Device name	Specify the terminal device name (also called the display name or the workstation ID) that the IBM System i should use for your session. If you leave this box blank, the IBM System i creates a device to use for your session.

The device name can be up to ten characters long. You can include any of the following characters as part of the value in the **Device name** box.

Character	Usage
*	Replaced by A, B, C, and so on to create a unique device name. If the entire alphabet is used, the generated device names continue with AA, AB, AC, and so on.
%	Replaced by P for printer sessions and S for display sessions.
=	Replaced by 1,2, 3, and so on to create a unique device name.
&COMPN	Replaced by the local workstation name, left-trimmed, if the generated name exceeds 10 characters.
&USERN	Replaced by the local user name, left-trimmed, if the generated name exceeds 10 characters.
+	Specifies right-trimming instead of left-trimming. Use with &COMPN or &USERN. This character can be placed anywhere in the string.

NOTE

◆ You can use only one string in combination with these characters. If you use separated strings, the second string is dropped. For example, %MyDevice= is valid. However, %My=Device is not valid, and will be treated by the system as if it were &My=.

◆ You cannot use both &COMPN and &USERN in the same string.

◆ To have Reflection generate unique device names automatically based on the special characters described above, the **Generate Device Names** setting must be enabled. In printer sessions, this setting is off by default. To enable it, see the "Generate Device Names" on page 612 topic.

Options

Automatically connect to the host	Select to establish a host connection as soon as the associated session document is opened.
When connection is terminated	Specify options for reconnecting after any disconnection that is not initiated from Reflection.

Choose	To have Reflection
Reconnect automatically	Attempt to reestablish the connection.
Prompt for reconnection	Prompt whether to attempt to reestablish the connection. (When No is selected, the session is left open and disconnected.)
Leave disconnected	Leave the session disconnected with the session open.
Close session automatically	Close the session.

Model

Model ID	Specify the model of the terminal or device type emulated by this session.

Related Topics

- "Configure Advanced Connection Settings Dialog Box" on page 329
- "Set Up Backup Connection Settings Dialog Box" on page 326
- "Configure Terminal Settings Dialog Box" on page 336

Set Up Backup Connection Settings Dialog Box

Getting there

1 Open a 5250 terminal session.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click 🗎.
TouchUx	Tap the Gear icon and then select 🗎 **Document Settings**.

2 Under **Host Connection**, click **Set up Backup Connection Settings**.

From this dialog box, you can specify the settings for one or more backup TN5250 connections. If your primary connection fails, these connections will be tried next, in the order they are listed.

Backup Hosts

Add a host to the Backup Host list by clicking the **Add** button. Use the **Move Up** and **Move Down** buttons to change the order in which the hosts are tried.

Enter Host (or System) Name or IP Address	Identify the host to which you will connect. Type the host name, alias, or numeric IP address.
	NOTE: Both IPv4 addresses (in the form 127.0.0.1) and IPv6 addresses (in the form 2001:0db8:3c4d:0015:0000:0000:abcd:ef12) are accepted.
Port	Type the host port or socket number that the session should use. This field accepts any number between 0 and 66,535 (default = 23).
Device name	Specify the terminal device name (also called the display name or the workstation ID) that the IBM System i should use for your session. If you leave this box blank, the IBM System i creates a device to use for your session.
	The device name can be up to ten characters long. You can include any of the following characters as part of the value in the **Device name** box.

Character	Usage
*	Replaced by A, B, C, and so on to create a unique device name. If the entire alphabet is used, the generated device names continue with AA, AB, AC, and so on.
%	Replaced by P for printer sessions and S for display sessions.
=	Replaced by 1,2, 3, and so on to create a unique device name.
&COMPN	Replaced by the local workstation name, left-trimmed, if the generated name exceeds 10 characters.
&USERN	Replaced by the local user name, left-trimmed, if the generated name exceeds 10 characters.
+	Specifies right-trimming instead of left-trimming. Use with &COMPN or &USERN. This character can be placed anywhere in the string.

NOTE

- ◆ You can use only one string in combination with these characters. If you use separated strings, the second string is dropped. For example, %MyDevice= is valid. However, %My=Device is not valid, and will be treated by the system as if it were &My=.

- ◆ You cannot use both &COMPN and &USERN in the same string.

- ◆ To have Reflection generate unique device names automatically based on the special characters described above, the Generate Device Names setting must be enabled. In printer sessions, this setting is off by default. To enable it, see the topic.

Host Connection Settings

When you enter more than one backup host, the connection options for each host are listed on a separate tab.

Options

Generate device names	When selected, Reflection automatically generates device names based on the value specified in the Device name field.
	For example, if the specified device name is %ABC=, Reflection generates the device name SABC1 for a display session. If SABC1 is already in use, Reflection tries SABC2, SABC3, and so on.
	Setting the device name to %123* generates the device name S123A for the first display session, S123B for the second session, and so on.
	When cleared, if the specified device name is in use, the session does not connect.

Model

Model ID	Specify the terminal (also known as a display station) you want to emulate.

Security

Security Settings	Secure data communications with SOCKS or SSL/TLS.

Related Topics

- ◆
- ◆
- ◆
- ◆

Configure Advanced Connection Settings Dialog Box

Getting there

1 Open a 5250 terminal session.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click .
TouchUx	Tap the Gear icon and then select **Document Settings**.

2 Under **Host Connection**, click **Configure Advanced Connection Settings**.

From this dialog box, you can define advanced TN5250 features.

Advanced 5250

Sign-on Options

Do Not Sign On Automatically	Select if you do not want to log on to the host as soon as you establish a connection. This is the default.
Automatically Sign On Using Windows Credentials	Select to log on to the host using your Windows user name and password. This option works in conjunction with IBM Enterprise Identity Mapping (EIM), which must be configured on your host computer.
Automatically Sign On Using Specified User ID and Password	Select to log on to the host using the specified user ID and password.

Connection Action

You can configure a session to run a macro, start an application, open a Web page, send an e-mail message, or perform a variety of other actions before or after it connects to the host.

Run a macro or other action before the initial connection	Select to run the connection action after the session file is opened but before the session initially connects to a host. (This action is performed even if the session is not configured to connect automatically.)
Select Action	Click to select an action to perform or a macro to run before you connect to the host. By default, the **Select Action** window opens at the screen for selecting a macro. If you prefer to perform a different action when your session connects, you can select other actions from the task pane.
Run a macro or other action after the initial connection	Select to run the connection action when the session initially connects to a host.
Select Action	Click to select an action to perform or a macro to run when you connect to the host.
Run when reconnecting	Select to run the connection action when the session initially connects to a host, and every time it reconnects to the host.

Security

Security Settings	Secure data communications with SOCKS or SSL/TLS.

Miscellaneous

Keep Alive

Send Keep Alive packets	Select to provide a constant check between your session and the host so that you become aware of connection problems as they occur.

Choose one of the three types of keep-alive packets:

Choose	To cause
System	The TCP/IP stack to keep track of the host connection. This method requires less system resources than Send NOP Packets or Send Timing Mark Packets. However, most TCP/IP stacks send Keep Alive packets infrequently.
Send NOP Packets	Reflection to periodically send a No Operation (NOP) command to the host. The host is not required to respond to these commands, but the TCP/IP stack can detect if there was a problem delivering the packet.

Send Timing Mark Packets	Reflection to periodically send a Timing Mark Command to the host to determine if the connection is still active. The host should respond to these commands. If Reflection does not receive a response or there is an error sending the packet, it shuts down the connection.
Keep Alive timeout in seconds	Select the interval between the keep-alive requests. The range of values is 1 to 9999 seconds; the default value is 600 seconds.

Telnet Location

Telnet location	(Optional) Type up to 41 characters of descriptive text to provide information about your session. For example, you might include your PC's location, computer name, or IP address.
	This features uses the SEND-LOCATION option supported under Telnet connections (RFC779).
	Reflection does not initiate a WILL SEND command unless you activate the Telnet location option by typing information in this box.

HLLAPI

Options

Short name	Select a HLLAPI short name to associate with this session. This value is used by a HLLAPI application to identify a host session. Any single capital letter (A-Z) can be used as a short name.
	By default, Reflection assigns the first available letter (A if no other sessions are running) and saves that short name value when you save your session document. If you open multiple sessions that have the same HLLAPI short name value, Reflection automatically reassigns the HLLAPI short name of each newly opened session using the next available letter.
	If your HLLAPI application requires a specific short name value, specify this value, then save your session document. If you run multiple sessions, you must ensure that sessions running at the same time do not require the same HLLAPI short name.
	If you want Reflection to generate new, arbitrary short name values for each new session, save all session documents with the HLLAPI short name set to A. Reflection will always set the HLLAPI short name to A for the first session, and will reset the short name to the next available letter for each subsequent session.
Long name	Enter a HLLAPI long name to associate with this session. A HLLAPI long name identifies the host session for the convenience of the user. It is not used by the HLLAPI application. The long name can be up to eight characters long and can include letters, numbers, and other characters.

Compatibility	If you are migrating from an Extra! or legacy Reflection product, and your application uses the default HLLAPI compatibility settings, simply select Reflection or Extra! from the **Compatibility** drop-down list. This configures the HLLAPI support in Reflection to match the default settings found in those applications.

If your application requires custom HLLAPI compatibility settings, select Custom from the **Compatibility** drop-down list. Once Custom is selected, you can enter a custom compatibility mask.

NOTE: Because of variations in the implementation of HLLAPI in previous products, when HLLAPI applications from Extra! and from previous versions of Reflection are run against Reflection, they may not behave exactly as they did when run against the product for which they were originally written. Even when you have selected the correct compatibility setting, minor differences may be seen in the status or return code reported by a handful of functions.

Custom compatibility mask

The possible numeric values for the custom compatibility mask styles are "bit masks" that contain separate bits of information about Reflection's HLLAPI configuration. Each style is equated to a decimal and hexadecimal value. A list of the styles and values is shown in the table below.

To create a compatibility mask, add the decimal or hexadecimal values of each style and enter the sum into the Custom Compatibility Mask field. Values can be entered in either decimal or hexadecimal format; however, when using hexadecimal values, replace the 0x at the front of the value with &H. For example, to use hexadecimal value 0x5380, enter &H5380 in the Custom Compatibility Mask field.

For example, to turn on the Propagate EAB (decimal value = 1), Input Inhibited Position (decimal value = 8), and Don't Wrap at PS End (decimal value = 512), add these three numbers (1 + 8 + 512 = 521) and enter the total into the Compatibility Mask field.

Style	Decimal Value	Hex Value
Propagate EAB	1	0x0001

When this bit is on, executing a Copy Presentation Space or Copy Presentation Space to String function, with the EAB and NOXLATE session parameters, causes each extended attribute specified at the start of a field to be copied to all characters in the field that do not have the corresponding extended attribute explicitly on. When this bit is off, the attribute is not copied to such characters. This bit applies only to 3270 sessions.

| **Query Host Update Protocol** | 2 | 0x0002 |

When this bit is on, Query Host Update functions report changes to the presentation space only if they are initiated by the host. When this bit is off, functions report changes initiated from the host or from the keyboard.

| **Input Inhibited Position** | 4 | 0x0004 |

This bit determines the position of the "input inhibited" indicator in the string returned from Copy OIA. When it is on, the indicator appears at position 9. When it is off, the indicator appears at position 5.

| **Copy PS to String Beyond End** | 8 | 0x0008 |

This bit determines what happens when the Copy Presentation Space to String function specifies a string that goes beyond the end of the presentation space. When it is on, no error is reported, the data from the position specified to the end of the presentation space is copied, and the remainder of the result string is set to binary zeros. When it is off, Reflection returns an error (APIPARAMETERERROR, value 2).

| **Wait a Second** | 16 | 0x0010 |

When this bit is on, HLLAPI waits one second beyond the last host-initiated presentation space modification before attempting to return a result. When it is off, HLLAPI does not wait. This affects functions Copy OIA, Query Host Update, Copy Presentation Space to String, and Copy Presentation Space.

| **Modify Protected Field** | 32 | 0x0020 |

When this bit is on, the Copy Presentation Space to String function can be used to copy to protected fields. When it is off, such copies are disallowed.

| **Translate 5250 Attributes to 3270** | 64 | 0x0040 |

When this bit is on, attributes copied by the HLLAPI application from the 5250 presentation space are translated to 3270 attributes. When it is off, Reflection returns 5250 attribute values (with the high order 2 bits on).

Always Blank	128	0x0080

When this bit is on, data characters found in the presentation space (by Copy Presentation Space to String or Copy Presentation Space) that can not be translated to ASCII are always translated to spaces. When it is off, the ATTRB setting is used to specify what should be done with such characters (if ATTRB is on, they are passed as their original value; if it is off, they are translated to spaces).

Transmit Modified Protected Fields	256	0x0100

This bit is relevant when HLLAPI modification of protected fields is allowed (see Modify Protected Field). When it is on, the modified protected field is not sent to the host in response to a read modified command. When it is off, the modified protected field is sent.

Don't Wrap at PS End	512	0x0200

This bit determines what happens if, on a copy from a string to the presentation space, the end of the presentation space is reached before the string is completely copied. If this bit is on, the operation terminates and returns an APITRUNCATED error. If it is off, copying continues at the beginning of the presentation space.

Error on Bad Escape	2048	0x0800

When this bit is on, undefined escape sequences passed to Send Key are reported by returning APIPARAMETERERROR. When it is off, such errors are ignored.

Terminate Send Key at AID	4096	0x1000

The default behavior for Send Key is to divide strings to be sent into segments terminated by an AID key, and then to send these segments sequentially, reporting an error only if the emulator objects (through input inhibited or busy status). When this bit is on, HLLAPI terminates the send after the first such segment, reporting an error if Error on Send Key Past AID is on. When this bit is off, HLLAPI does not report an error under such circumstances.

Error on Send Key Past AID	8192	0x2000

When this bit is on, the HLLAPI application reports an error if Send Key continues to send characters after a transmitted AID key. When it's off, the application does not report an error under such circumstances.

Return Zero Length Fields	16384	0x4000

If this bit is set, Find Field Position (31) returns APIOK and position of next field (in the position parameter) for a zero length field. Otherwise, it returns APIZEROLENFIELD and a 0 in the position parameter.

Caching Off	32768	0x8000

When set on, this bit disables the caching mechanism that increases performance. If you are having problems with your application synching with the Reflection screen, try turning on this bit. After enabling this bit, you may notice some degradation in HLLAPI performance.

Old Flashpoint	65536	0x10000

Flashpoint versions 3.1 and earlier expect consecutive CopyPS calls to include or not include attributes regardless of how attributes are set. Turning on this bit makes HLLAPI accept this behavior.

DOS ASCII Converter	131072	0x20000

This bit converts a HLLAPI character to DOS ASCII format.

Extra! OIA Values	262144	0x40000

When this bit is on, the Copy OIA returns OIA buffer values that match the Extra! values instead of the default Reflection values.

Rumba Style	297	0x0129

The Reflection HLLAPI configuration matches the default settings found in Rumba.

Extra! Style	21380	0x5384

The Reflection HLLAPI configuration matches the default settings found in Extra!.

Related Topics

-

Select Host Code Page Dialog Box (5250)

Getting there

1 Open a 5250 terminal session.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click .
TouchUx	Tap the Gear icon and then select **Document Settings**.

2 Under **Terminal Configuration**, click **Select Host Code Page**.

Host Code Page

Language/Code page	Select the language and associated host code page to be used by your session. If you are not sure which language and code page to use, check with your system administrator. The default is US English, code page 037.

Related Topics

♦ "Change the UI Language" on page 219

♦ "Editing a Host Code Page" on page 311

Configure Terminal Settings Dialog Box

Getting there

1 Open a 5250 terminal session.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click .
TouchUx	Tap the Gear icon and then select **Document Settings**.

2 Under **Terminal Configuration**, click **Configure Terminal Settings**.

From this dialog box, you can set input and other options for your 5250 terminal.

Display

Use dots to separate columns	Select to use periods as column separators. This is the default unless you are running a Japanese operating system.
Use vertical lines to separate columns	Select to use vertical lines as column separators. This is the default if you are running a Japanese version of the product.
Disable text blinking	When selected, text set to blink by the host does not blink.
Blink rate	Specifies the speed at which text set to blink by the host blinks.
Status line	Select the type of status line to display at the bottom of the terminal window when your session is connected.

This option	Uses
3488 Status Line	Symbols to represent various conditions and is based on the status line you see on newer 5250 terminals from IBM.
5250 Status Line	Character pairs to represent various conditions. The characters are always shown but appear in inverse video when the condition is true.
	For example, when the system is not available, the letters SA appear in regular video. However, when the system is available, the letters appear in inverse video.
Debug Status Line	The 5250 datastream for troubleshooting. If you contact Micro Focus Technical Support, you may be asked to use the Debug Status Line to help diagnose the problem. This option is for users with an intimate knowledge of the 5250 datastream.

Input field underlining	Specifies whether to underline fields that allow input. You can set options to never underline, allow the host to control underlining, or always underline.

Input

Word Wrap

Select the way you want word wrap to be handled. If word wrap is enabled, text is wrapped from one entry field to the next on a word boundary if possible; if word wrap is disabled, text continues from one entry field to the next without regard to word boundaries.

Host controls word wrap	The host is allowed to enable or disable word wrap on a per-field basis.
Enable word wrap	Word wrap is enabled for all entry fields regardless of host settings.
Disable word wrap	Word wrap is disabled for all entry fields regardless of host settings.

Type Ahead

Select the way you want type-ahead to be handled. If type-ahead is enabled, typed characters are buffered while the host is not ready for data; if type-ahead is disabled, typed characters are ignored until the host is ready for data.

Host controls type-ahead	The host is allowed to enable or disable type-ahead.
Enable type-ahead	Type-ahead is enabled regardless of host settings.
Disable type-ahead	Type-ahead is disabled regardless of host settings.

Keyboard Error

Select the way you want keyboard errors to be handled.

No auto reset when a keyboard error occurs	Before you can resume data entry, you must press Reset to clear the error message.		
Auto reset when a keyboard error occurs	The next key you press clears the error and attempts to execute the keystroke as follows:		
		If	**This occurs**
		The cursor is in a valid input field and the key is a data key	The data is entered there if it is valid data for that field (for example, a numeric character in an input field that only accepts numbers).
			Otherwise, the cursor is moved to the next valid input field, and if the data is valid for that field, it is entered there.
		The cursor is in a valid input field and the key is a function key	The key operation is executed.
			Otherwise, the cursor is moved to the next valid input field, and the key is ignored.
		The current screen contains no valid input fields	An error message appears with each keystroke you press, and no keystrokes are executed.
Auto reset without error message	You don't need to press Reset to clear a keyboard error. No error is reported and the next key you press attempts to execute the keystroke as follows:		
		If the cursor	**This occurs**
		Is in a valid input field	The key is ignored. This is true for both data keys and function keys.

	Is not in a valid input field and the key is a data key	The cursor is moved to the next valid input field, and if the data is valid for that field, it is entered there.
	Is not in a valid input field and the key is a function key	The cursor is moved to the next valid input field, and the key is ignored.
	Use this value with caution, because it prevents notification of keyboard errors.
Beep when keyboard error is detected	You'll hear a beep when you encounter a keyboard error. **NOTE:** If you select **Auto reset without error message**, it's recommended that you also select this option, so that you'll know when a keyboard error occurs.

Mouse

Mouse cursor shape	Select whether to display the mouse cursor as an arrow, an i-beam, or a rectangle.
Rectangular selection	Dragging the mouse across an area selects only the text within that area. When this option is cleared (unchecked), the selection wraps to line ends.

Miscellaneous

Preserve entry mode	When selected, the session remains in extended graphics mode or hexadecimal mode indefinitely after you enter either mode. Use the same keystroke to exit these modes as you use to enter them. When this option is not selected, the session automatically exits extended graphics mode after you enter a graphic or diacritical character, and automatically exits hexadecimal mode after you enter a hexadecimal pair.
Enable host beep	When selected, beeps sent by the host are sounded.
Enable AID field exit mode	When selected, unrestricted sending of AID key values (F1-F24 only) to the host from restricted input fields is allowed.
Support double-byte character set	Select to use Asian languages such as Japanese, Chinese, and Korean in your terminal session.

Related Topics

Set Up Display Settings

Getting there

1 Open a 5250 terminal session.

2 If the user interface is not in **Classic** mode, set it to **Classic** as follows:

    2a Open the Reflection Workspace Settings dialog box. The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **File** menu or the Reflection button, choose **Reflection Workspace Settings**.
Reflection Browser	On the Reflection menu, choose **Settings** and then **Reflection Workspace Settings**.
TouchUx	Tap the Gear icon and then select **Reflection Workspace Settings**.

    2b Under **Workspace Settings**, select **Configure User Interface**.

    2c In the **User interface mode** list, select **Classic**.

    2d Close and reopen the Reflection Workspace.

3 On the **Options** menu, choose **Settings.**

4 Under **Terminal Configuration**, click **Set up Display Settings**.

NOTE: "Caption" settings configuration is available for all 3270/5250 sessions when in "Classic" User Interface mode.

Caption	Specifies the string that appears in the Reflection title bar.
	This string is also displayed on the taskbar when Reflection is running. If Reflection is running but minimized, the configured string will be displayed on the taskbar. Type a predefined shortcut option, or enter up to 260 characters in the box. The predefined shortcuts and options are:

Shortcut	Option
&w	Micro Focus
&r	Product Name
&f	Session File Name
&s	Session Type
&t	Transport
&h	Host Name
&d	Date

&c	Connection Status (whether you are connected and over what transport)
&v	Assigned Device Name (relevant only for 5250 sessions that use an assigned Device Name)
&l	Assigned LU Name (relevant only for 3270 sessions that use an assigned LU Name)
&&	A single Ampersand

For example, if you set the Caption to &s - &t - &c, you should see something like "IBM 5250 Terminal - Telnet - *hostname* via Telnet" in the Reflection title bar or on the taskbar, assuming Reflection is running but not minimized. (The exact text depends on your configuration.) The default is &f - &r - &s.

Show Menu Bar   Display the menu and toolbar in Classic mode.

NOTE: When this option is unselected, you can display the menu by clicking the Reflection button [icon] and then choosing **Show Menu Bar**.

Show Status Bar   Display the status bar in Classic mode.

VT Sessions

This section includes detailed information on configuring your VT sessions.

In this Section

Related Topics

VT Document Settings Dialog Box

Getting there

1 Open the Create New Document dialog box.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	From the Quick Access Toolbar, click the **New Document** 🗋 button.
TouchUx	Tap the Folder icon and then under **File**, select 🗋 **New**.

2 From the **Create New Document** dialog box, select a VT terminal session, and then click **Create**.

Connection

Telnet	Select to use your PC as a virtual terminal over a TCP/IP connection. When Telnet is the selected protocol, you can configure secure connections using SSL/TLS.
Secure Shell	Select for secure, encrypted communications between a trusted host and your PC over an insecure network. When you select Secure Shell, all connections between your PC and the remote host(s) are encrypted, protecting the data sent between these machines.
Rlogin	Select to use your PC as a virtual terminal over a TCP/IP connection.
Enter Host (or System) Name or IP Address	Identify the host to which you will connect. Type the host name, alias, or numeric IP address. **NOTE:** Both IPv4 addresses (in the form 127.0.0.1) and IPv6 addresses (in the form 2001:0db8:3c4d:0015:0000:0000:abcd:ef12) are accepted.
Port	Type the host port or socket number that the session should use. This field accepts any number between 0 and 66,535 (default = 23).
User Name	Type a name that identifies you or your PC to the host. This option is enabled only for Secure Shell or Rlogin connections.
SSH configuration	Type a descriptive name to label these connection settings, making them available for use with other sessions. If you leave this field blank, and make changes to any secure shell configuration, Reflection saves the configuration scheme using the value from the **Host name/IP address** field. (See "SSH Configuration Schemes" on page 485.)

Terminal

Terminal Type	Select the terminal to emulate. This specifies the codes generated by the numeric keypad, the interpretation of control functions, and the response to terminal identification requests. (Values under **Terminal** automatically reset when you choose a terminal type.)

Support graphics	Select to support the Tektronix 401x terminal type or the Remote Graphics Instruction Set (ReGIS) by DEC. REGIS includes the following features:

- Up to 16 colors
- Shading with selected patterns and polygon fill
- Rubberband cursors
- Rotated and italicized characters
- Mouse support
- A scaled graphic showing the complete ReGIS screen (800x480 pixels) on the physical display

Keyboard map	Specify the keyboard map to use with this session.
Configure additional settings	Select to open a page from which you can customize host connection, terminal configuration, and other settings for this session.
	When selected, the session does not auto-connect. This allows you to modify settings before connecting to the session.

Related Topics

ReGIS Graphics Support

For accurate ReGIS and sixel graphics emulation using Reflection, on the **Graphics** tab from the **Terminal Setup** dialog box, the **Terminal type** should be set to one of the four graphics terminal types: VT240, VT241, VT330, or VT340.

NOTE

- The VT240 and VT330 are monochrome graphics terminals, providing up to four shades of gray at once.
- The VT241 and VT340 are color graphics terminals; the VT241 provides up to four different colors at once, while the VT340 provides up to 16 different colors.
- Setting your display to 256 colors is highly recommended.

All four graphics terminals support ReGIS. However, each terminal differs slightly in its implementation of ReGIS. Reflection should be set for the same type of terminal as that of the host graphics program.

A host program may need to determine the graphics capabilities of Reflection. It does so by requesting the **Terminal ID** (which is set on the **Emulation** tab from the **Terminal Setup** dialog box). For accurate graphics emulation, the **Terminal ID** should be set to the type of terminal the host expects to find: VT240, VT241, VT330, or VT340 (the default is VT320).

NOTE: Changing the **Terminal type** resets all associated settings (that is, any setting from the **Terminal Setup** dialog box or the **Advanced Options** dialog box).

Related Topics

- "Graphics Tab (Terminal Setup Dialog Box)" on page 377
- "Select Terminal Type Dialog Box" on page 359

Configure Connection Settings Dialog Box (VT)

Getting there

1 Open a VT terminal session.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ⬛.
TouchUx	Tap the Gear icon and then select ⬛ **Document Settings**.

2 Under **Host Connection**, click **Configure Connection Settings**.

From this dialog box, you can specify the settings for a VT connection.

Connection Method

Network	Configure a host connection through a network.
Serial Port	Configure a host connection through a serial port on your PC.
Modem	Configure a host connection through a modem. The modem must first be configured in Windows.

Network

These options are available only when you have selected **Network** under **Connection Method**.

Network Connection Type

Telnet	Select to use your PC as a virtual terminal over a TCP/IP connection. When Telnet is the selected protocol, you can configure secure connections using SSL/TLS.
Secure Shell	Select for secure, encrypted communications between a trusted host and your PC over an insecure network. When you select Secure Shell, all connections between your PC and the remote host(s) are encrypted, protecting the data sent between these machines.
Rlogin	Select to use your PC as a virtual terminal over a TCP/IP connection.

Connection Options

Host name/IP address	Identify the host to which you will connect. Type the host name, alias, or numeric IP address.
	NOTE: Both IPv4 addresses (in the form 127.0.0.1) and IPv6 addresses (in the form 2001:0db8:3c4d:0015:0000:0000:abcd:ef12) are accepted.
User name	Type a name that identifies you or your PC to the host.
	This option is enabled only for Secure Shell or Rlogin connections.
SSH configuration scheme	Type a descriptive name to label these connection settings, making them available for use with other Secure Shell sessions.
	If you leave this field blank, and make changes to any connection settings, Reflection saves the configuration scheme using the value from the **Host name/IP address** field.
Handle SSH User authentication in terminal window	For Secure Shell connections, display user name and password prompts in the terminal window instead of in a dialog box.
Security	Secure data communications with Secure Shell, SOCKS, or SSL/TLS.
More Settings	Configure additional settings.

Serial Port

These options are available only when you have selected **Serial Port** under **Connection Method**.

Serial port to use	Reflection detects available serial ports on your PC and displays them here.
Parity	Set the parity for data transmission to and from the serial device on this port.
	This setting determines whether a parity bit is generated for each character transmitted. Parity is used to detect errors in data transmission; the number preceding the slash indicates the number of data bits sent.
	To use the multinational character set or 8-bit controls, **Parity** must be set to one of the values that offers 8-bit controls. If your communications link generates parity, and you set **Parity** to **8/None**, multinational characters appear on your screen. In this case, set **Parity** to either **8/Even** or **8/Odd**.
Baud	Set the rate at which Reflection transmits and receives data through the selected serial port.
	The baud rate setting must match the baud rate of your direct connection.
More Settings	Configure additional settings.

Modem

These options are available only when you have selected **Modem** under **Connection Method**.

Modem to use	Reflection detects modems configured on your PC and displays them here.
Phone number	Type the phone number you want the modem to dial when connecting. The number must adhere to the rules of your modem.
Use country code and city code	Select this option if you want to specify a country code and city code (or area code) for the number you are dialing.
	Clear this option if you do not want to use the **Country code**, **City code**, and **Current location** options.
Country code	Type the country code for the country you are calling.
City code	Type the city code or area code for the location you are calling.
Current location	Select the previously defined location from which you are calling. These locations are defined from the **Dialing Properties** dialog box.
Dialing Properties	Add, modify, or remove a location from the **Current location** list.
More Settings	Configure additional settings.

Connection Action

You can configure a session to run a macro, start an application, open a Web page, send an e-mail message, or perform a variety of other actions before or after it connects to the host.

Run a macro or other action before the initial connection	Select to run the connection action after the session file is opened but before the session initially connects to a host. (This action is performed even if the session is not configured to connect automatically.)
Select Action	Click to select an action to perform or a macro to run before you connect to the host. By default, the **Select Action** window opens at the screen for selecting a macro. If you prefer to perform a different action when your session connects, you can select other actions from the task pane.
Run a macro or other action after the initial connection	Select to run the connection action when the session initially connects to a host.
Select Action	Click to select an action to perform or a macro to run when you connect to the host.
Run when reconnecting	Select to run the connection action when the session initially connects to a host, and every time it reconnects to the host.

Connection Options

Automatically connect to the host	Select to establish a host connection as soon as the associated session document is opened.
Allow exit while connected	Select to allow closing the workspace when a session is connected to a host.
When connection is terminated	Specify options for reconnecting after any disconnection that is not initiated from Reflection.

Choose	To have Reflection
Reconnect automatically	Attempt to reestablish the connection.
Prompt for reconnection	Prompt whether to attempt to reestablish the connection. (When No is selected, the session is left open and disconnected.)
Leave disconnected	Leave the session disconnected with the session open.
Close session automatically	Close the session.

Related Topics

- "General Tab (More Settings Telnet Dialog Box)" on page 347
- "Advanced Tab (More Settings Telnet Dialog Box)" on page 355
- "Options Tab (More Settings Telnet Dialog Box)" on page 349
- "More Settings Secure Shell Dialog Box" on page 351
- "More Settings RLogin Dialog Box" on page 352
- "More Settings Serial Port Dialog Box" on page 354

General Tab (More Settings Telnet Dialog Box)

Getting there

1 Open a VT terminal session and then open the Settings dialog box.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ![icon].
TouchUx	Tap the Gear icon and then select ![icon] **Document Settings**.

2 Under **Host Connection**, click **Configure Connection Settings**.

3 Under **Connection Method**, select **Network**.

4 Under **Network Connection Type**, select **Telnet**.

5 Under **Connection Options**, click the **More Settings** button.

The options are:

TCP port	Most Telnet hosts wait for an incoming connection on TCP Port 23. If your host uses a different port, type that number here.
Parity	This setting determines whether a parity bit is generated for each character transmitted. Parity is used to detect errors in data transmission; the number preceding the slash indicates the number of data bits sent.
	To use the multinational character set or 8-bit controls, **Parity** must be set to one of the values that offers 8-bit controls. If your communications link generates parity, and you set **Parity** to **8/None**, multinational characters appear on your screen. In this case, set **Parity** to either **8/Even** or **8/Odd**.
Terminal type	To override the default terminal, select or type a value here.
	In general, you control the following characteristics when you change terminal types:

- Which screen control sequences the host sends to Reflection to format the screen.
- The position of the cursor.
- Which characters to display in a host application.

	If you're having trouble running a host application, the negotiation between Reflection and the host might be wrong. If you enter a terminal type that the host does not recognize, Reflection reverts to a list of default values until one is found that the host supports.
	This option is not available if you are connecting to a network modem over Telnet.
Timeout	Specify the number of milliseconds Reflection should attempt to make a connection before timing out. The maximum value is 65535. The timeout period begins after host name resolution has taken place. This means an additional delay, usually a few seconds beyond the value specified.
	When this is set to 0 (the default), Reflection timeout behavior is determined by your Windows operating system.
Use emulation terminal ID	Select to force Reflection to ignore the **Terminal type** setting and instead use the value from the **Terminal ID** setting on the **Emulation** tab from the **Terminal Setup** dialog box.
Use threaded I/O	Select to send communication calls to an independent thread that handles IO (Input/Output) processing, thus improving performance.

Related Topics

Options Tab (More Settings Telnet Dialog Box)

Getting there

1 Open a VT terminal session and then open the Settings dialog box.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ⬚.
TouchUx	Tap the Gear icon and then select ⬚ **Document Settings**.

2 Under **Host Connection**, click **Configure Connection Settings**.

3 Under **Connection Method**, select **Network**.

4 Under **Network Connection Type**, select **Telnet**.

5 Under **Connection Options**, click the **More Settings** button.

The options are:

Initiate option negotiation	Specifies whether certain connection options, including whether to always request a binary mode connection, should be negotiated when the Telnet connection is established. When cleared, connections to some hosts on the Internet are expedited so that Reflection does not attempt to initiate negotiations for Telnet options.
Trace negotiation	Select to cause Telnet to write the negotiation process for the various Telnet options to the screen. This is useful for debugging.
Request binary (Option 0)	Telnet defines a 7-bit data path between the host and the terminal (or, in this case, Reflection). This type of data path is not compatible with certain national character sets and some file transfer protocols (for example, Xmodem and Zmodem). Fortunately, many hosts allow for 8-bit data without zeroing the 8th bit, which resolves this problem. However, In some cases, it may be necessary to force the host to use an 8-bit data path by selecting this option. **NOTE:** This option is not available when **Initiate option negotiation** is cleared.
Local echo (Option 1)	Select the way you want Reflection to respond to remote echo from a Telnet host:

Specify	To have Reflection
Automatic (default)	Attempt to negotiate remote echo, but do as the host commands.
Yes	Negotiate local echo with the host, but always echo.
No	Negotiate remote echo with the host, but not echo.

Ctrl-Break character	Select what happens when you press Ctrl+Break. By default, Reflection sends the **Interrupt process** sequence to the host. If your host expects a **Telnet break** sequence, then select this option instead.
Set host window size (Option 31)	Select to send the number of rows and columns to the Telnet host whenever they change, so that the host can properly control the cursor if the window size is changed.
Dynamic terminal size (Option 31)	Select to support dynamic update of the number of rows and columns in the display when the user resizes the terminal window. Your Telnet server and application must also support NAWS (Negotiate About Window Size), otherwise display problems can occur.
	Note: You can quickly determine the screen size of the terminal window whenever you hover the mouse cursor over the Row and Column indicator (located in the left corner of the status bar). Under Telnet and Secure Shell connection types, the tooltip will also feature "Auto" if **Dynamic terminal size** is selected.
Linemode (Option 34)	Line mode allows Reflection to store characters in a buffer until a carriage return is entered, at which point, the characters are sent to the host in one packet (instead of sending each single character as an individual packet).
	Line mode is useful when long network delays are an issue, and allows you to reduce costs on networks that charge on a per packet basis.

Select	To use line mode when
RFC Compliant	Your host supports it, and it gets negotiated during connect.
During Local Echo	The host tells Reflection to do the echoing.
When Not in SGA	The host does not Suppress Go Ahead.

All options other than **RFC Compliant** are known as "faux" line mode.

Suppress local echo (Option 45)	Select to suppress the local echoing of characters to the display.
Renegotiate echo	Some hosts require a period of time to initialize a connection before accepting a request by the client to recognize and perform a Local Echo. Select this option to let Reflection attempt a second negotiation of the Local Echo option following the initialization period.

Related Topics

- "Configure Connection Settings Dialog Box (VT)" on page 344

More Settings Secure Shell Dialog Box

Getting there

1 Open a VT terminal session.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ![icon].
TouchUx	Tap the Gear icon and then select ![icon] **Document Settings**.

2 Under **Host Connection**, click **Configure Connection Settings**.

3 Under **Connection Method**, select **Network**.

4 Under **Network Connection Type**, select **Secure Shell**.

5 Under **Connection Options**, click the **More Settings** button.

The options are:

Parity	This setting determines whether a parity bit is generated for each character transmitted. Parity is used to detect errors in data transmission; the number preceding the slash indicates the number of data bits sent.

To use the multinational character set or 8-bit controls, **Parity** must be set to one of the values that offers 8-bit controls. If your communications link generates parity, and you set **Parity** to **8/None**, multinational characters appear on your screen. In this case, set **Parity** to either **8/Even** or **8/Odd**. |
| **Baud** | Select the rate at which Reflection transmits and receives data through the network connection. |
| **Terminal type** | To override the default terminal, select or type a value here.

In general, you control the following characteristics when you change terminal types:

- Which screen control sequences the host sends to Reflection to format the screen.
- The position of the cursor.
- Which characters to display in a host application.

If you're having trouble running a host application, the negotiation between Reflection and the host might be wrong. If you enter a terminal type that the host does not recognize, Reflection reverts to a list of default values until one is found that the host supports. |
| **Timeout** | Specify the number of milliseconds Reflection should attempt to make a connection before timing out. The maximum value is 65535. The timeout period begins after host name resolution has taken place. This means an additional delay, usually a few seconds beyond the value specified.

When this is set to 0 (the default), Reflection timeout behavior is determined by your Windows operating system. |
| **Session limits** | Select the maximum number of sessions you want to allow for a Telnet connection. |

Close on disconnect	Select to close your session document when you disconnect from the host.
Set host window size	Select to send the number of rows and columns to the Telnet host whenever they change, so that the host can properly control the cursor if the window size is changed.
Dynamic terminal size	Select to support dynamic update of the number of rows and columns in the display when the user resizes the terminal window. Your Telnet server and application must also support NAWS (Negotiate About Window Size), otherwise display problems can occur.
	Note: You can quickly determine the screen size of the terminal window whenever you hover the mouse cursor over the Row and Column indicator (located in the left corner of the status bar). Under Telnet and Secure Shell connection types, the tooltip will also feature "Auto" if **Dynamic terminal size** is selected.

Related Topics

More Settings RLogin Dialog Box

Getting there

1 Open a VT terminal session.

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click .
TouchUx	Tap the Gear icon and then select **Document Settings**.

2 Under **Host Connection**, click **Configure Connection Settings**.

3 Under **Connection Method**, select **Network**.

4 Under **Network Connection Type**, select **Rlogin**.

5 Under **Connection Options**, click the **More Settings** button.

The options are:

TCP port	When connecting to a host via Rlogin, most hosts wait for an incoming connection on TCP Port 513. If your host uses a different port, type that number here.

Parity	This setting determines whether a parity bit is generated for each character transmitted. Parity is used to detect errors in data transmission; the number preceding the slash indicates the number of data bits sent.
	To use the multinational character set or 8-bit controls, **Parity** must be set to one of the values that offers 8-bit controls. If your communications link generates parity, and you set **Parity** to **8/None**, multinational characters appear on your screen. In this case, set **Parity** to either **8/Even** or **8/Odd**.
Baud	Select the rate at which Reflection transmits and receives data through the network connection.
Terminal type	To override the default terminal, select or type a value here.
	In general, you control the following characteristics when you change terminal types:
	◆ Which screen control sequences the host sends to Reflection to format the screen.
	◆ The position of the cursor.
	◆ Which characters to display in a host application.
	If you're having trouble running a host application, the negotiation between Reflection and the host might be wrong. If you enter a terminal type that the host does not recognize, Reflection reverts to a list of default values until one is found that the host supports.
Timeout	Specify the number of milliseconds Reflection should attempt to make a connection before timing out. The maximum value is 65535. The timeout period begins after host name resolution has taken place. This means an additional delay, usually a few seconds beyond the value specified.
	When this is set to 0 (the default), Reflection timeout behavior is determined by your Windows operating system.
Session limits	Select the maximum number of sessions you want to allow for a Telnet connection.
Close on disconnect	Select to close your session document when you disconnect from the host.

Related Topics

◆ "Configure Connection Settings Dialog Box (VT)" on page 344

More Settings Serial Port Dialog Box

Getting there

1 Open a VT terminal session.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click .
TouchUx	Tap the Gear icon and then select **Document Settings**.

2 Under **Host Connection**, click **Configure Connection Settings**.

3 Under **Connection Method**, select **Serial Port**.

4 Under **Serial Port**, click the **More Settings** button.

NOTE: Modem pacing is set from the **More Settings - Modem** dialog box.

Pacing

It is possible for Reflection to transmit data to a serial device faster than the device can process it, or for a serial device to transmit data to Reflection faster than Reflection can process it.

Should this continue for too long, the slower system's buffer overflows and data is lost. If the serial device recognizes the XON/XOFF handshake, you can prevent the buffer from overflowing by keeping this value set to **Xon/Xoff**.

Xon/Xoff transmit pacing works as follows:

- When the receive buffer has a limited amount of space left, an XOFF (DC3) character is sent as a signal to stop transmitting.

- After processing most of the backlog of characters in the receive buffer, an XON (DC1) character is sent as a signal to resume transmission.

  The two systems continue in this stop-and-go fashion until all the data has been transmitted.

  If **Hardware** is selected, the RTS and CTS pins on the RS-232 serial cable control data flow.

  When both the **Receive** and **Transmit** options under **Pacing** are set to **None** and you're emulating a VT series terminal, Hold Session (VtF1) has no effect.

Transmit	Select a flow control method to use when Reflection transmits data to a serial device on this port.
Receive	Select a flow control method to use when the serial device on this port transmits data to Reflection.

Char transmit delay	It is possible for Reflection to send data to the host faster than the host can receive it. For example, if you paste text from the Clipboard into a host editor such as EDT, you may overrun the host's buffer.
	By setting a delay between characters, you can specify how long Reflection should wait after each character when transmitting blocks of characters to the host.
	This delay also affects character transmission during file transfers. Setting a value of 3 at 9600 baud lowers the effective speed of data transmission to about 2400 bits per second.
	On a VMS host, setting the terminal's HOSTSYNC characteristic can also help prevent overrunning the host's buffer when pasting data. To do this, enter the following command at the DCL prompt: `SET TERMINAL/HOSTSYNC`.
	For backward compatibility, you can enter a value for character delay of up to 255. However, the maximum in Reflection always reverts to 100.
Line transmit delay	Set the amount of time Reflection should wait after transmitting a carriage return character (the line delimiter) before transmitting the next line.
	This setting also affects the delay between frames during file transfer using the WRQ/Reflection protocol. Assigning a delay may help if you are experiencing file transfer problems over an X.25 connection.
Use threaded I/O	Select to send communication calls to an independent thread that handles IO (Input/Output) processing, thus improving performance.

Related Topics

- “Configure Connection Settings Dialog Box (VT)” on page 344
- “Configure Serial Device Port Dialog Box” on page 592

Advanced Tab (More Settings Telnet Dialog Box)

Getting there

1 Open a VT terminal session and then open the Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click 🗋.
TouchUx	Tap the Gear icon and then select 🗋 **Document Settings**.

2 Under **Host Connection**, click **Configure Connection Settings**.

3 Under **Connection Method**, select **Network**.

4 Under **Network Connection Type**, select **Telnet**.

5 Under **Connection Options**, click the **More Settings** button.

The options are:

Session limits	Select the maximum number of sessions you want to allow for a Telnet connection.
Terminal default	Type a value to send as a backup to the Telnet server if the server requests this information, and doesn't recognize the current value set for **Terminal type**.
	NOTE: During negotiations, some hosts that could successfully connect using your preferred terminal type skip over this value during negotiations and connect using the backup value specified by **Terminal default**. To correct this behavior, set **Terminal default** to an empty value ("").
Bind to local port	Select to choose a specific local port for Reflection to connect through to communicate with the host.
	If this option is cleared, Reflection will use the next available port.
Local port	Specify a local port.
	If this option is set to zero, Reflection uses the next available port.
Send LF after CR	A "true" Telnet host expects to see a `CrNu` (carriage return/null) character sequence to indicate the end of a line sent from a terminal (in this case, Reflection). There are some hosts on the Internet that are not true Telnet hosts, and they expect to see a `Lf` (line feed) character following the `Cr` at the end of a line. If you're connecting to this type of Telnet host, select this option.
Telnet location	(Optional) Type up to 41 characters of descriptive text to provide information about your session. For example, you might include your PC's location, computer name, or IP address.
	This features uses the SEND-LOCATION option supported under Telnet connections (RFC779).
	Reflection does not initiate a WILL SEND command unless you activate the **Telnet location** option by typing information in this box.

Related Topics

- "Configure Connection Settings Dialog Box (VT)" on page 344

More Settings Modem Dialog Box

Getting there

1 Open a VT terminal session.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ![icon].
TouchUx	Tap the Gear icon and then select ![icon] **Document Settings**.

2 Under **Host Connection**, click **Configure Connection Settings**.

3 Under **Connection Method**, select **Modem**.

4 Under **Modem**, click the **More Settings** button.

The settings in this dialog box control the modem currently selected in the **Modem to use** list. If you switch to another modem, these settings will then apply to that modem.

Connection mode	Select an action to take when making a modem connection.

Select	To do this
CALL	Dial the remote host specified in the **Phone number** box.
AUTO-ANSWER	Connect to the modem and wait for the first ring of an incoming call before answering.
ANSWER	Connect to the modem and immediately answer any incoming call.
DIRECT	Connect to the modem so you can enter modem commands in the terminal window.
DIALBACK	Dial the remote host specified in the **Phone number** box, disconnect, then wait for a return call. Use this setting if you are using a security dialback host.

Baud rate	Set the rate at which Reflection transmits and receives data through the selected modem.
	The default baud rate is that specified in Windows Control Panel, from the **Modem Properties** dialog box, defined when you installed your modem.
	When connecting to a host via modem, you may need to select a different baud rate. The maximum baud rate is a function of many factors, such as the type of modem you have and the quality and length of the communications line.

Parity	Set the parity for data transmission through this connection.
	This setting determines whether a parity bit is generated for each character transmitted. Parity is used to detect errors in data transmission; the number preceding the slash indicates the number of data bits sent.
	To use the multinational character set or 8-bit controls, **Parity** must be set to one of the values that offers 8-bit controls. If your communications link generates parity, and you set **Parity** to **8/None**, multinational characters appear on your screen. In this case, set **Parity** to either **8/Even** or **8/Odd**.

Pacing

It is possible for Reflection to transmit data to a serial device faster than the device can process it, or for a serial device to transmit data to Reflection faster than Reflection can process it.

Should this continue for too long, the slower system's buffer overflows and data is lost. If the serial device recognizes the XON/XOFF handshake, you can prevent the buffer from overflowing by keeping this value set to **Xon/Xoff**.

Xon/Xoff transmit pacing works as follows:

 * When the receive buffer has a limited amount of space left, an XOFF (DC3) character is sent as a signal to stop transmitting.
 * After processing most of the backlog of characters in the receive buffer, an XON (DC1) character is sent as a signal to resume transmission.

   The two systems continue in this stop-and-go fashion until all the data has been transmitted.

Transmit	Select a flow control method to use when Reflection transmits data to a serial device on this port.
Receive	Select a flow control method to use when the serial device on this port transmits data to Reflection.
Char transmit delay	It is possible for Reflection to send data to the host faster than the host can receive it. For example, if you paste text from the Clipboard into a host editor such as EDT, you may overrun the host's buffer.
	By setting a delay between characters, you can specify how long Reflection should wait after each character when transmitting blocks of characters to the host.
	This delay also affects character transmission during file transfers. Setting a value of 3 at 9600 baud lowers the effective speed of data transmission to about 2400 bits per second.
	On a VMS host, setting the terminal's HOSTSYNC characteristic can also help prevent overrunning the host's buffer when pasting data. To do this, enter the following command at the DCL prompt: `SET TERMINAL/HOSTSYNC`.
	For backward compatibility, you can enter a value for character delay of up to 255. However, the maximum in Reflection always reverts to 100.
Line transmit delay	Set the amount of time Reflection should wait after transmitting a carriage return character (the line delimiter) before transmitting the next line.
	This setting also affects the delay between frames during file transfer using the WRQ/Reflection protocol. Assigning a delay may help if you are experiencing file transfer problems over an X.25 connection.

Related Topics

◆ "Configure Connection Settings Dialog Box (VT)" on page 344

Select Terminal Type Dialog Box

Getting there

1 Open a VT terminal session.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click .
TouchUx	Tap the Gear icon and then select **Document Settings**.

2 Under **Terminal Configuration**, click **Select Terminal Type**.

Terminal Type

Terminal Type	Select the terminal to emulate. This specifies the codes generated by the numeric keypad, the interpretation of control functions, and the response to terminal identification requests. (Values under **Terminal** automatically reset when you choose a terminal type.)

Graphics

Support graphics	Select to support the Tektronix 401x terminal type or the Remote Graphics Instruction Set (ReGIS) by DEC. REGIS includes the following features:

- ◆ Up to 16 colors
- ◆ Shading with selected patterns and polygon fill
- ◆ Rubberband cursors
- ◆ Rotated and italicized characters
- ◆ Mouse support
- ◆ A scaled graphic showing the complete ReGIS screen (800x480 pixels) on the physical display

Terminal Settings

Terminal Setup	Set values specific to the type of terminal you are emulating. Changing the **Terminal type** resets all associated settings (that is, any setting from the **Terminal Setup** dialog box or the **Advanced Options** dialog box).

Related Topics

Emulation Tab for VT Terminal Types

Getting there

1 Open a VT terminal session and then open the Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click .
TouchUx	Tap the Gear icon and then select **Document Settings**.

2 Under **Terminal Configuration**, click **Configure Terminal Settings**.

Set values specific to the type of terminal you are emulating. Changing the **Terminal type** resets all associated settings (that is, any setting from the **Terminal Setup** dialog box or the **Advanced Options** dialog box). These options apply to most VT terminal types.

Emulation Options

Host character set	Select a character set to load as the default when a soft reset is performed; or when you invoke the DECSTR sequence. The **Host character set** may also be specified by the Select Character Set (SCS) sequence.
PC character set	If you need the DOS character set for file transfer or printing, select **DOS** from this list.

Terminal ID	Determines the response that Reflection sends to the host after a primary device attributes (DA) request. This response lets the host know what terminal functions it can perform. This setting is independent of the **Terminal type** setting.
	When set to **WRQ**, Reflection responds to a primary DA request with the set of features it supports. The responses that Reflection sends for each terminal ID are listed in the VT Terminal Reference pdf file.
	Reflection does not support the VT420 feature of multiple sessions over a single serial line.
	Terminal IDs that end with the letter J (such as VT101J) indicate Japanese terminal support. These terminal IDs cause Reflection to send the correct DA response for Japanese terminals, and to size the DBCS (double-byte) characters appropriately.
Online	Select to have Reflection function as a terminal (also called "remote mode").
	Clear this option to enter local mode. In local mode, Reflection does not attempt to communicate with a host computer. Characters entered from the keyboard appear on the screen, but are not transmitted to the host; nor is any data received from the host (for example, notification of a mail message).
	This value is not saved with your session document.
New line	Select to send both a carriage return and line feed when you press Enter (known as new line mode). When Reflection receives a line feed, form feed, or vertical tab, it moves the cursor to the first column of the next line. When this option is cleared (linefeed mode), the Enterkey sends only a carriage return. A line feed, form feed, or vertical tab received from the host moves the cursor down one line in the current column.
	If lines on the display keep getting overwritten (that is, the host is not sending a line feed along with a carriage return), select this option. If this option is selected, but the host does not expect to receive a line feed with each carriage return, lines are double-spaced on the display.
Autowrap	Select to make characters wrap to the next line automatically when the cursor reaches the right margin of the display.
	This setting is different from the VAX host's terminal wrap characteristic, which is set with the following DCL command:
	`SET TERMINAL/[NO]WRAP`
	The host command determines whether characters wrap automatically when they reach the maximum terminal width set by the host's `SET TERMINAL/WIDTH` command (instead of using the right margin of the display, like this setting).
	◆ If terminal wrap is set on the host, characters wrap when they reach the maximum terminal width, regardless of whether **Autowrap** is selected.
	◆ If terminal wrap is not set and **Autowrap** is cleared, new characters overwrite the character at the right margin until a carriage return is entered.

Use ANSI color	Select to use ANSI color in the Reflection terminal display under Reflection VT emulations. When selected, the **ANSI Color Mapping** section of the **Modify Theme** dialog box becomes enabled.
Treat ambiguous Unicode characters as wide	This setting is available only when using the UTF-8 host character set.
	Some Unicode characters resolve to either narrow or wide, depending upon the context in which they are used. In East Asian typography, these characters are usually display as wide.
Advanced	Click to open the **Advanced Options** dialog box, from which you can configure advanced options for this terminal type.
	NOTE: This button is not available for BBS-ANSI, SCO-ANSI, or VT-UTF8 emulation.

Related Topics

- "Advanced Options Dialog Box for VT Terminal Types" on page 365
- "Select Terminal Type Dialog Box" on page 359

Emulation Tab for IBM 3151 Terminals

Getting there

1 Open a VT terminal session and then open the Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ⬚.
TouchUx	Tap the Gear icon and then select ⬚ **Document Settings**.

2 Under **Terminal Configuration**, click **Select Terminal Type**.

3 Under **Terminal Type**, under **Other**, select **IBM 3151**.

4 Under **Terminal Settings**, click **Terminal Setup**.

IBM 3151 Emulation options

Host character set	Select a character set to load as the default when a soft reset is performed; or when you invoke the DECSTR sequence. The **Host character set** may also be specified by the Select Character Set (SCS) sequence.
PC character set	If you need the DOS character set for file transfer or printing, select **DOS** from this list.
Insert Character	Select the way you want the INSERT key to behave.

Select	To cause the INSERT key to
Insert Space	Insert a Space character.

Mode Toggle	Toggle between Insert mode and Replacement mode.

Tab	Select the way you want the TAB key to behave.

Select	To move the cursor to
Column	The next tab stop.
Field	The next field of a formatted screen.

Received LF	Select how you want a received line feed to be interpreted: as a line feed (LF), or as a carriage return followed by a line feed (LFCR).

Online	Select to have Reflection function as a terminal (also called "remote mode"). Clear this option to enter local mode. In local mode, Reflection does not attempt to communicate with a host computer. Characters entered from the keyboard appear on the screen, but are not transmitted to the host; nor is any data received from the host (for example, notification of a mail message). This value is not saved with your session document.

New line	Select to send both a carriage return and line feed when you press Enter (known as new line mode). When Reflection receives a line feed, form feed, or vertical tab, it moves the cursor to the first column of the next line. When this option is cleared (linefeed mode), the Enterkey sends only a carriage return. A line feed, form feed, or vertical tab received from the host moves the cursor down one line in the current column. If lines on the display keep getting overwritten (that is, the host is not sending a line feed along with a carriage return), select this option. If this option is selected, but the host does not expect to receive a line feed with each carriage return, lines are double-spaced on the display.

Autowrap	Select to make characters wrap to the next line automatically when the cursor reaches the right margin of the display. This setting is different from the VAX host's terminal wrap characteristic, which is set with the following DCL command: `SET TERMINAL/[NO]WRAP` The host command determines whether characters wrap automatically when they reach the maximum terminal width set by the host's `SET TERMINAL/WIDTH` command (instead of using the right margin of the display, like this setting). ♦ If terminal wrap is set on the host, characters wrap when they reach the maximum terminal width, regardless of whether **Autowrap** is selected. ♦ If terminal wrap is not set and **Autowrap** is cleared, new characters overwrite the character at the right margin until a carriage return is entered.

Advanced	Click to open the **Advanced Options** dialog box, from which you can configure advanced options for this terminal type.

Related Topics

- "Advanced Options Dialog Box for IBM 3151 Terminals" on page 367
- "Select Terminal Type Dialog Box" on page 359

Emulation Tab for Wyse Terminal Types

Getting there

1 Open a VT terminal session and then open the Settings dialog box.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ⬚.
TouchUx	Tap the Gear icon and then select ⬚ **Document Settings**.

2 Under **Terminal Configuration**, click **Select Terminal Type**.

3 Under **Terminal Type**, select a Wyse terminal type.

4 Under **Terminal Settings**, click **Terminal Setup**.

Wyse Emulation options

Host character set	Select a character set to load as the default when a soft reset is performed; or when you invoke the DECSTR sequence. The **Host character set** may also be specified by the Select Character Set (SCS) sequence.
PC character set	If you need the DOS character set for file transfer or printing, select **DOS** from this list.
Received CR	Select how you want a received carriage return to be interpreted, as a carriage return alone (CR) or a carriage return followed by a line feed (CRLF).
Block terminator	Select the end-of-transmission delimiter for block sends. This is typically set by the host application. The default value, **US/CR**, sends a US at the end of a line and a CR at the end of a page/block. **CRLF/ETX** sends a CR and LF at the end of a line and an ETX at the end of a page.
Return key	Select the character the RETURN key transmits.
Enter key	Select the character the ENTER key transmits.
Online	Select to have Reflection function as a terminal (also called "remote mode").
	Clear this option to enter local mode. In local mode, Reflection does not attempt to communicate with a host computer. Characters entered from the keyboard appear on the screen, but are not transmitted to the host; nor is any data received from the host (for example, notification of a mail message).
	This value is not saved with your session document.

New line	Select to send both a carriage return and line feed when you press Enter (known as new line mode). When Reflection receives a line feed, form feed, or vertical tab, it moves the cursor to the first column of the next line. When this option is cleared (linefeed mode), the Enterkey sends only a carriage return. A line feed, form feed, or vertical tab received from the host moves the cursor down one line in the current column.
	If lines on the display keep getting overwritten (that is, the host is not sending a line feed along with a carriage return), select this option. If this option is selected, but the host does not expect to receive a line feed with each carriage return, lines are double-spaced on the display.
Autowrap	Select to make characters wrap to the next line automatically when the cursor reaches the right margin of the display.
	This setting is different from the VAX host's terminal wrap characteristic, which is set with the following DCL command:
	`SET TERMINAL/[NO]WRAP`
	The host command determines whether characters wrap automatically when they reach the maximum terminal width set by the host's `SET TERMINAL/WIDTH` command (instead of using the right margin of the display, like this setting).
	◆ If terminal wrap is set on the host, characters wrap when they reach the maximum terminal width, regardless of whether **Autowrap** is selected.
	◆ If terminal wrap is not set and **Autowrap** is cleared, new characters overwrite the character at the right margin until a carriage return is entered.
Recognize del	Select this option if you want Reflection to interpret a received `DEL` character.
Advanced	Click to open the **Advanced Options** dialog box, from which you can configure advanced options for this terminal type.

Related Topics

- "Advanced Options Dialog Box for Wyse Terminal Types" on page 369
- "Select Terminal Type Dialog Box" on page 359

Advanced Options Dialog Box for VT Terminal Types

Getting there

1 Open a VT terminal session and then open the Settings dialog box.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ⬜.
TouchUx	Tap the Gear icon and then select ⬜ **Document Settings**.

2 Under **Terminal Configuration**, click **Configure Terminal Settings**.

These options change depending on the terminal type selected.

VT features

User features locked	Select to lock the following items so that they cannot be changed by the host:
	◆ Tab stops
	◆ Keyboard lock
	◆ Screen background
	◆ Scrolling speed
	◆ Auto repeat
User-defined keys locked	Select to prevent the host from clearing or redefining user-defined keys.
	This value is not saved with your session document.
Status line	Select a status line type.

National Replacement Characters

National Replacement Set	Available only when, from the **Terminal Setup** dialog box, **ISO-Latin 1** or **DEC Supplemental** is specified as the Host character set.
	Select one of the 12 national replacement character sets built into Reflection. National replacement sets are used in 7-bit operating environments, when characters from the supplemental character sets cannot be accessed by 8-bit codes. Each national replacement set replaces certain characters from the ASCII set with accented characters and symbols for a specific national language.
Use NRC (7-bit) Set	In an 8-bit operating environment, you can enable a national replacement set with this option.

Answerback message

Answerback message	If the host expects an answer in response to an ENQ character, type the answer here.
Insert special characters	Select to allow escape sequences and ASCII control codes in the message (for example, press Enter to include a CR character).

Auto answerback	Select to cause the answerback message to be sent to the host automatically after a communications line connection. You may transmit the answerback message at any time by pressing Alt+F7 (this method of sending the message replaces the VT320 keystroke Ctrl+Break).
Clear	Click to clear the answerback message.
Conceal	Click to replace the message with the word <Concealed>. Once a string is concealed, there is no way to unconceal it; you have to replace the text by typing new text, or click **Clear** to start again.
Serial device to host	Select to maintain a serial connection to the configured port and send any characters received from this serial connection to the existing host connection. This setting is typically enabled by the host application when it is required.
Configure	Click to select and configure a serial port.
	The **Configure** button from the **Terminal Setup Advanced Options** dialog box is equivalent to the **Configure** button from the **Logging Settings** dialog box. You can use the button from either dialog box to configure your serial device port.
Custom DA response	Select to enter a custom Device Attributes (DA) response and then type a sequence for the response in the field below.
	The terminal sends this string in response to a primary device attributes request.

Related Topics

- "Emulation Tab for VT Terminal Types" on page 360
- "Select Terminal Type Dialog Box" on page 359
- "Configure Serial Device Port Dialog Box" on page 592

Advanced Options Dialog Box for IBM 3151 Terminals

Getting there

1 Open a VT terminal session and then open the Settings dialog box.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click [icon].
TouchUx	Tap the Gear icon and then select [icon] **Document Settings**.

2 Under **Terminal Configuration**, click **Select Terminal Type**.

3 Under **Terminal Type**, under **Other**, select **IBM 3151**.

4 Under **Terminal Settings**, click **Terminal Setup**.

The options are:

IBM 3151 features

Null Suppress	Send trailing nulls to the system. Clear this option to convert trailing nulls to spaces before sending them to the system.
Send Null Suppress	When in Block mode, Reflection won't send null characters in terminal memory in a Send operation (Send line, Send page, Send memory). Clear this option to have null characters sent as spaces (in Block mode only).
Line Turnaround Char	Define the LineTurnAround (LTA) character.

Specify	To define the LTA as
CR (default)	A carriage return
ETX	End Of Text character, ASCII 3
EOT	An End Of Transmission Character, ASCII 4
DC3	A Device Control 3 (XOFF), ASCII 19

Force Insert Line	Insert a null line at the selected line. This happens when an insert line operation is performed by either Reflection or the host under IBM 3151 emulation.
	Select this option to force off the last line on a screen when a line insertion operation is performed and there is no null line that can be deleted to accommodate the insertion.
Force Insert Char	Insert a null character at the selected character. This happens when an insert character operation is performed by either Reflection or the host under IBM 3151 emulation.
	Select this option to force a character off a row (or off the end of the screen if Autowrap is on) when a character insertion operation is performed and there is no null character that can be deleted to accommodate the insertion.

Answerback message

Answerback message	If the host expects an answer in response to an ENQ character, type the answer here.
Insert special characters	Select to allow escape sequences and ASCII control codes in the message (for example, press Enter to include a CR character).
Auto answerback	Select to cause the answerback message to be sent to the host automatically after a communications line connection. You may transmit the answerback message at any time by pressing Alt+F7 (this method of sending the message replaces the VT320 keystroke Ctrl+Break).
Clear	Click to clear the answerback message.

Conceal	Click to replace the message with the word <Concealed>. Once a string is concealed, there is no way to unconceal it; you have to replace the text by typing new text, or click **Clear** to start again.
Serial device to host	Select to maintain a serial connection to the configured port and send any characters received from this serial connection to the existing host connection. This setting is typically enabled by the host application when it is required.
Configure	Click to select and configure a serial port.
	The **Configure** button from the **Terminal Setup Advanced Options** dialog box is equivalent to the **Configure** button from the **Logging Settings** dialog box. You can use the button from either dialog box to configure your serial device port.

Related Topics

- ◆ "Emulation Tab for IBM 3151 Terminals" on page 362
- ◆ "Emulation Tab for Wyse Terminal Types" on page 364
- ◆ "Configure Serial Device Port Dialog Box" on page 592

Advanced Options Dialog Box for Wyse Terminal Types

Getting there

1 Open a VT terminal session and then open the Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ⬚.
TouchUx	Tap the Gear icon and then select ⬚ **Document Settings**.

2 Under **Terminal Configuration**, click **Select Terminal Type**.

3 Under **Terminal Type**, select a Wyse terminal type.

4 Under **Terminal Settings**, click **Terminal Setup**.

The options are:

Wyse Features

Label lines	The terminal decides how many label lines are visible by how many display rows are requested. Reflection allows you to always have two. If only one label line is visible, use the Shift key to display the second line.
Status line	Select a status line type.

Answerback message

Answerback message	If the host expects an answer in response to an ENQ character, type the answer here.
Insert special characters	Select to allow escape sequences and ASCII control codes in the message (for example, press Enter to include a CR character).
Auto answerback	Select to cause the answerback message to be sent to the host automatically after a communications line connection. You may transmit the answerback message at any time by pressing Alt+F7 (this method of sending the message replaces the VT320 keystroke Ctrl+Break).
Clear	Click to clear the answerback message.
Conceal	Click to replace the message with the word <Concealed>. Once a string is concealed, there is no way to unconceal it; you have to replace the text by typing new text, or click **Clear** to start again.
Serial device to host	Select to maintain a serial connection to the configured port and send any characters received from this serial connection to the existing host connection. This setting is typically enabled by the host application when it is required.
Configure	Click to select and configure a serial port.
	The **Configure** button from the **Terminal Setup Advanced Options** dialog box is equivalent to the **Configure** button from the **Logging Settings** dialog box. You can use the button from either dialog box to configure your serial device port.

Related Topics

- "Emulation Tab for Wyse Terminal Types" on page 364
- "Select Terminal Type Dialog Box" on page 359
- "Configure Serial Device Port Dialog Box" on page 592

Keyboard & Mouse Tab (Terminal Setup Dialog Box)

Getting there

1 Open a VT terminal session and then open the Settings dialog box.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ⬚.
TouchUx	Tap the Gear icon and then select ⬚ **Document Settings**.

2 Under **Terminal Configuration**, click **Configure Terminal Settings**.

Keyboard modes

Auto repeat	Select to make most keys repeat when pressed. The Shift, Return, and Ctrl keys do not auto repeat.
Break enabled	Select to enable the Break function. When cleared, both the Break command and the VtF5 (Break) keystroke (Ctrl+Break) are disabled.
Local echo	Select to cause each character typed at the keyboard to be immediately displayed on the screen. When you're communicating with the host computer, each character typed at the keyboard is transmitted to the host. Most host systems (for example, a VAX running VMS) immediately send the same character back to the terminal (that is, echo the character). The character is not displayed on the screen until it is received back from the host.
	When you're online and you select this option, each character is sent two places: directly to display memory (the screen), and to the host computer. On an echoing host system, this means that each character you type appears twice on the screen. Select this option only when communicating with host systems that do not echo each typed character; for example, some public networks.

Bells

Margin bell	Select to have your computer beep when the cursor is eight characters from the right margin.
Warning bell	Select to have your computer beep when the ASCII bell character (Bel, decimal 7) is received from the host or entered from the keyboard.
	To disable the format bell (which beeps, for example, when Reflection encounters an unprotected field), clear the **Warning bell** option.

Terminal keys

VT backspace sends	Select the function that you want your Backspace key to send.
	You can also remap the Backspace key using the Keyboard Mapper. Doing so has no effect on the **VT backspace sends** option. However, this option is affected when you remap the VtBackArrow terminal keystroke.

Cursor keys	This option controls the characters that the four Arrow keys (on both the numeric and editing keypad) transmit. This setting is typically set by the host and is not saved to the session document.
	If the Arrow keys aren't working properly, it may mean that this option remained incorrectly set to **Application** when a host program terminated abnormally. If changing this setting back to **Normal** doesn't fix the problem with the Arrow keys, check the value set for **Terminal ID**, and verify that it matches the type of terminal the host expects. The VT52 setting, for instance, sends different cursor key codes than the other (ANSI) modes.
	NOTE: This feature is unavailable for WYSE emulation.
Keypad	This option controls the characters that the numeric keypad keys transmit. This setting is typically set by the host and is not saved to the session document.
	If the number or PF keys aren't working properly, it may mean that this option remained incorrectly set to **Application** when a host program terminated abnormally. If changing this setting back to **Numeric** doesn't fix the numeric keypad, check the VT operating level Mode and make sure it matches that of the host. The VT52 setting, for instance, sends different keypad codes than the other (ANSI) modes.
	NOTE: This feature is unavailable for WYSE emulation.

Keyboard shortcuts

NOTE: Settings in the Keyboard Mapper override these options.

Standard File and Edit menu shortcuts	Select to enable the following keyboard shortcuts:

PC keystroke	Terminal function
Ctrl+A	Select All
Ctrl+C	Copy
Ctrl+F	Find
Ctrl+Shift+F	Find Next
Ctrl+O	Open File
Ctrl+P	Print File
Ctrl+V	Paste
Ctrl+X	Cut

Hold Screen shortcuts	Select to have Reflection use Ctrl+Q to start and Ctrl+S to stop the processing of data from the host.
	Clear **Hold Screen shortcuts** if you use a host application (such as EMACS) that requires the use of the Ctrl+S and Ctrl+Q characters. Clearing this option allows the Ctrl+S keystroke to send to the host a Ctrl+S character (ASCII decimal 19), and the Ctrl+Q keystroke to send to the host a Ctrl+Q character (ASCII decimal 17).

Mouse shortcuts

Always copy selected text to the clipboard	Text selected using the left mouse button and drag action is copied to the Clipboard when you release the mouse button.
Right-click pastes clipboard text	The contents of the Clipboard are pasted into Reflection at the cursor location when the right mouse button is clicked.
	NOTE: Settings in the Mouse Mapper override these options.
Middle button pastes clipboard text	The contents of the Clipboard are pasted into Reflection at the cursor location when the middle mouse button is clicked.
	NOTE: Settings in the Mouse Mapper override these options.
Rectangular Selection	Dragging the mouse across an area selects only the text within that area. When this option is cleared (unchecked), the selection wraps to line ends.

Related Topics

- ◆ "Select Terminal Type Dialog Box" on page 359
- ◆ "Specifying a Custom Keyboard Map" on page 272
- ◆ "Specifying a Mouse Map" on page 275

Keyboard & Mouse Tab for IBM 3151 Terminals

Getting there

1 Open a VT terminal session and then open the Settings dialog box.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ⬚.
TouchUx	Tap the Gear icon and then select ⬚ **Document Settings**.

2 Under **Terminal Configuration**, click **Configure Terminal Settings**.

Keyboard modes

Auto repeat	Select to make most keys repeat when pressed. The Shift, Return, and Ctrl keys do not auto repeat.
Break enabled	Select to enable the Break function. When cleared, both the Break command and the VtF5 (Break) keystroke (Ctrl+Break) are disabled.
Local echo	Select to cause each character typed at the keyboard to be immediately displayed on the screen. When you're communicating with the host computer, each character typed at the keyboard is transmitted to the host. Most host systems (for example, a VAX running VMS) immediately send the same character back to the terminal (that is, echo the character). The character is not displayed on the screen until it is received back from the host.
	When you're online and you select this option, each character is sent two places: directly to display memory (the screen), and to the host computer. On an echoing host system, this means that each character you type appears twice on the screen. Select this option only when communicating with host systems that do not echo each typed character; for example, some public networks.

Bells

Margin bell	Select to have your computer beep when the cursor is eight characters from the right margin.
Warning bell	Select to have your computer beep when the ASCII bell character (`Bel`, decimal 7) is received from the host or entered from the keyboard.
	To disable the format bell (which beeps, for example, when Reflection encounters an unprotected field), clear the **Warning bell** option.

Terminal keys

Select how the following keys act when pressed under IBM 3151 emulation.

Send Key	The default value transmits the entire page to the host. Select **Line** to have Reflection transmit only the selected line to the host.
Return Key	The default value transmits a newline request to the host. Select **Field** to have Reflection move to the next field of a formatted screen.
Enter Key	The default value acts as a Send key. Select **Return** to have the Enter key act as a Return key.
Backspace Key	Select a value to send when the Backspace key is pressed.

The values available represent the unshifted/shifted states you can choose from. For example, selecting **BS/DEL** means pressing Backspace sends a Backspace to the host. Pressing the Shift key and then pressing Backspace will send a Delete to the host.

This value	Designates
BS	Backspace, ASCII 8.
DEL	Delete, ASCII 127.
CAN	Cancel, ASCII 24.

Keyboard shortcuts

NOTE: Settings in the Keyboard Mapper override these options.

Standard File and Edit menu shortcuts	Select to enable the following keyboard shortcuts:

PC keystroke	Terminal function
Ctrl+A	Select All
Ctrl+C	Copy
Ctrl+F	Find
Ctrl+Shift+F	Find Next
Ctrl+O	Open File
Ctrl+P	Print File
Ctrl+V	Paste
Ctrl+X	Cut

Hold Screen shortcuts	Select to have Reflection use Ctrl+Q to start and Ctrl+S to stop the processing of data from the host.
	Clear **Hold Screen shortcuts** if you use a host application (such as EMACS) that requires the use of the Ctrl+S and Ctrl+Q characters. Clearing this option allows the Ctrl+S keystroke to send to the host a Ctrl+S character (ASCII decimal 19), and the Ctrl+Q keystroke to send to the host a Ctrl+Q character (ASCII decimal 17).

Mouse shortcuts

Always copy selected text to the clipboard	Text selected using the left mouse button and drag action is copied to the Clipboard when you release the mouse button.
Right-click pastes clipboard text	The contents of the Clipboard are pasted into Reflection at the cursor location when the right mouse button is clicked.
	NOTE: Settings in the Mouse Mapper override these options.
Middle button pastes clipboard text	The contents of the Clipboard are pasted into Reflection at the cursor location when the middle mouse button is clicked.
	NOTE: Settings in the Mouse Mapper override these options.
Rectangular Selection	Dragging the mouse across an area selects only the text within that area. When this option is cleared (unchecked), the selection wraps to line ends.

Related Topics

Tabs Tab (Terminal Setup Dialog Box)

Getting there

1 Open a VT terminal session and then open the Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ⬚.
TouchUx	Tap the Gear icon and then select ⬚ **Document Settings**.

2 Under **Terminal Configuration**, click **Configure Terminal Settings**.

Tab Stops

Tab stops	Use the mouse, cursor keys, or Spacebar to move the scroll bar to the desired column and click; a T appears on the ruler. Repeat the procedure until all tabs are set. If you're in 132-column mode, use the scroll bars to move beyond the 81st column to set a tab stop.
	To clear a single tab stop, click the tab position with the mouse (each click of the mouse toggles between setting a tab stop and clearing it).
Clear All	Click to clear all tabs set on the tab ruler.
	The left margin is always an implicit tab stop and is not affected by **Clear All**.
Set Every	To set tab stops at equidistant positions, enter a number in the box and click **Set Every**.

Graphics Tab (Terminal Setup Dialog Box)

Getting there

1 Open a VT terminal session and then open the Settings dialog box.

The steps depend on your .

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ⬚.
TouchUx	Tap the Gear icon and then select ⬚ **Document Settings**.

2 Under **Terminal Configuration**, click **Configure Terminal Settings**.

ReGIS

Terminal type	Select which terminal is emulated and how many shades or colors are available in ReGIS:
	◆ The VT240 and VT330 are monochrome graphics terminals, providing up to four shades of gray at once.
	◆ The VT241 and VT340 are color graphics terminals; the VT241 provides up to four different colors at once, while the VT340 provides up to 16 different colors.
	This value is independent of the settings for **Terminal ID** on the **Emulation** tab.

Graphics output cursor	Clear this option to hide the graphics output cursor.
	ReGIS displays two types of graphic cursors: an input cursor and an output cursor. The input cursor appears when ReGIS is waiting for graphics input, such as a cursor position report. You can position the input cursor with the mouse or the Arrow keys. A graphics output cursor appears when ReGIS is waiting for commands from the host (or from the ReGIS command line).
	Displaying the graphics output cursor can also be controlled by the ReGIS command `S(C<n>)`. The ReGIS command option controls the style of the graphics output cursor.
Macrograph reports	Clear this option to disable macrograph reporting for security or other reasons.
	A macrograph is a way to define and store a set of ReGIS commands as a single character; that is, as a graphics macro. By default, ReGIS can report the contents of a specific macrograph.

Sixel

Print mode	Select how sixel data is sent to the host or a Digital printer.

Select	To do this
Compress	Print an image pixel-for-pixel.
Rotate	Rotate the image 90 degrees (from portrait to landscape orientation).
	If you want the actual output to print rotated, from the **Print Setup** dialog box, select **Landscape** as the **Orientation** option.
Expand	Print each pixel twice as wide and twice as high.
	Expanded printing applies only when sending sixel data to the host (selected by the **Destination**), not to a PC printer.

Destination	When you print a graphics image using the ReGIS hard copy command, the image can be sent either to the host or a Digital printer.
	When the graphics image is sent to the host, it is sent as a stream of sixel data. The host must be ready to accept the data; for example, by collecting it in a file.
	When the image is sent to a host printer, it is printed as a bitmap image. If **Bypass Windows print driver** is selected from the **Print Setup** dialog box, a sixel data stream is sent to the printer (assuming you are printing to a Digital printer).

Graphics level	With this option, you can match Reflection to Digital printer capabilities, such as aspect ratio, horizontal grid size, background printing, and color printing. The sixel data string sent to the host varies based on the graphics level for details about the sixel data format.
	This setting applies only when sending sixel data to the host or a Digital printer when **Bypass Windows printer driver** is selected from the **Print Setup** dialog box.
	This setting also affects saving display sixels from the **Save Display As** dialog box.
Color printing	Select Color or Mono (black and white) printing.
	This setting applies only when sending sixel data to the host or a Digital printer when **Bypass Windows printer driver** is selected from the **Print Setup** dialog box.
	This setting also affects saving display sixels from the **Save Display As** dialog box.
Color specification	If you are printing in color, select the color coordinate system to use for color sixel printing.
	This setting applies only when sending sixel data to the host or a Digital printer when **Bypass Windows printer driver** is selected from the **Print Setup** dialog box.
	This setting also affects saving display sixels from the **Save Display As** dialog box.
Scrolling	A sixel is a vertical column of six pixels used to display graphic images. When scrolling is enabled, the sixel image begins at the current text position. A sixel image will scroll the display when the image reaches the bottom margin of the display (if it doesn't fit, the image may also scroll off the top of the display). A graphics newline character is sent immediately after the sixel dump, and the text cursor is set at the same position as the sixel cursor when you exit sixel mode.
	When this option is cleared, the sixel image begins at the upper left of the display. When the image reaches the bottom margin, the display does not scroll, and additional sixel commands are ignored. Upon exiting sixel mode, the text cursor is set at the same position as when sixel mode was entered.

Tektronix

CR processing	When you select CR-LF, a linefeed character is appended to each carriage return character. This is useful when you're operating in local mode (when, from the **Terminal Setup** dialog box, on the **Emulation** tab, the **Online** option is cleared).
LF processing	When you select LF-CR, a carriage return character is appended to each linefeed character. This is useful when you're operating in local mode (when, from the **Terminal Setup** dialog box, on the **Emulation** tab, the **Online** option is cleared).
Del processing	Reflection interprets DEL characters as valid ASCII characters. To have Reflection ignore DEL characters, select **Ignored**.
GIN terminator	Select which character or characters act as a terminator for cursor address information.
Destructive overwrite	By default, a character typed over another one in Tektronix emulation does not erase the first one: the second character is superimposed on the first. Select this option to specify that you want a character cell blanked out before a character is drawn.

Printing

Print graphics	Select this option to print graphics along with the text when sending sixels to the host or to a Digital printer.
	This setting also affects saving display sixels from the **Save Display As** dialog box.
Print background	Select whether to print the graphics image with or without the background color when sending sixels to the host or a Digital printer.
	Clear this option to print to a printer that can print only a black and white bitmap, and no shades of gray. The colors of the screen image are inverted for printing. This makes light-colored graphics print as black images on white paper. If you're printing 16-color graphics, the resulting images may be unpredictable as a 16-color image must be converted to a 2-color (black and white) bitmap. This applies to sixels generated as well as graphics printed on Windows printers.
	This setting also affects saving display sixels from the **Save Display As** dialog box.

Copying

VGA dithering	Select to cause bitmaps copied to the Clipboard to be dithered to standard VGA colors. This is useful for pasting graphic images into Windows applications that are not palette-aware (for example, Windows Paint).

Select the level of dithering to be applied when a 256-color image is pasted into the terminal window from the Clipboard. Because Reflection emulates a 16-color terminal, it uses an algorithm to determine exactly how colors should be mapped. The best dithering choice for an image may vary depending on the image.

Select	To produce this
Half	A pasted image that takes a middle course between the **None** and **Full** values.
Full	The most accurate color translation. However, the pasted image could have a grainy, textured appearance.
None	A pasted image with a color specified for each individual pixel. This option produces the crispest image. However, there may be no distinct color boundaries.
	NOTE: Selecting **None** as the level of VGA dithering does not have the same effect as clearing the **VGA dithering** check box. The state of the check box controls whether the image is converted to a VGA-displayable image when it is copied — if the check box is cleared, the exact image is copied (including its exact colors). This works well when pasting graphics into applications that are palette-aware (such as Photoshop).
	For applications that are not palette-aware (such as Windows Paint), select this check box and pick a dithering option (explained above) that determines how Reflection processes the pixels.

Copy background	When cleared, bitmaps copied to the Clipboard are edited so that the background color is set to white, and all near-white colors are set to black. This is useful for pasting graphic images into word processing documents.

Related Topics

◆ "ReGIS Graphics Support" on page 343

◆ "Select Terminal Type Dialog Box" on page 359

Set Up Display Settings Dialog Box

Getting there

1 Open a VT terminal session.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ![icon].
TouchUx	Tap the Gear icon and then select ![icon] **Document Settings**.

2 Under **Terminal Configuration**, click **Set Up Display Settings**.

The options are:

Display Memory

Display memory contains both the information visible on the display and (if **Enable scrollback** is selected) information that has scrolled off of the display. It is a log of what has recently been sent from the host to the PC. Display memory stores only text; if you have graphics on the display, they are not scrolled into display memory.

Memory blocks (8K/block)	Type the number of memory blocks to allocate for display memory.
	The default is 9 blocks of 8 kilobytes each, or 72K of display memory. This holds approximately 22 pages of display memory when each line is exactly 80 characters long.
	The number of bytes you are currently using is calculated on each character of text; you'll have more "pages" of display memory when your text lines do not run all the way out to the right margin.
Enable scrollback	With scrollback enabled, the session maintains a buffer of lines that have scrolled off the terminal screen. This allows the user to scroll back through this buffer and read or copy it. A real terminal does not have this extra memory and clearing this selection will accurately emulate the behavior of the terminal.
	NOTE: This setting does not affect VT420 or Wyse paged memory.
Compress blank lines	Select to save room in display memory by compressing multiple blank lines into a single blank line.
Save display before clearing	Select to move the data on the display into display memory when you or the host clear the display. Otherwise, the data is discarded.
Save from scrolling regions	When a scrolling region is set on the display, by default, text that scrolls out of the scrolling region is not saved in display memory. If you want the text from the scrolling region moved into display memory, select this option.
	If a scrolling region is set by a text editor, selecting this option can cause display memory to fill quickly; every time you scroll down your document, text that scrolls off the top of the display is moved into display memory. For most situations, it's best to leave this option cleared.

Scrolling

Smooth scrolling   Select to display all lines in sequence as they are received from the host, even when doing so results in a delay between receiving a line and displaying it.

Jump scrolling   Select to display incoming lines of data as quickly as they are received from the host, even when doing so results in some lines being "jumped over" and not displayed. The jumped-over lines are captured in the display memory, so you can still see them by scrolling back through display memory.

You'll notice the effect of this setting only when data from the host is arriving faster than it can be displayed.

Jump scroll speed   Select the number of lines to "jump over" if it becomes necessary to catch up with data coming in from the host.

Control Characters

The VT terminal character set includes 65 control characters with decimal values 0-31 and 127-159.

Interpret control characters   Select to interpret control characters as they are received from the host. For example, the carriage return character moves the cursor to the left margin.

Display control characters   Select to display control characters rather than interpret them. This lets you see exactly which characters are received from the host and which control characters are generated by the keyboard.

Mouse

Mouse cursor shape   Select whether to display the mouse cursor as an i-beam or an arrow.

Dimensions

Number of rows   Specify the number of lines on the display, not including the status line. This defines the display size, and the host can position and write characters anywhere within this area. The maximum number of rows you can enter depends on the display resolution; the higher the screen resolution your video adapter provides, the more rows you can fit on the screen.

When you change the number of rows, characters are scaled vertically to fit the desired number of rows, or lines, in the terminal window. The display is erased (all of display memory is cleared) before the new setting takes effect.

Setting rows here does not change the number of rows the host can recognize.

Number of characters per row	Specify the number of characters per row (that is, columns) in the scrolling region in the terminal window (between 80 and 999).

When you change the number of characters per row, the font size is adjusted in an attempt to fit all the characters in the terminal window. If all the characters cannot be displayed, a horizontal scroll bar appears to the right of the status bar.

Setting the number of characters per row here does not change the number of characters per row the host can recognize.

NOTE: Changing the number of characters per row in the display automatically changes the number of columns used by your printer in the **Columns per row** box in the **Page Options** dialog box.

Options

NOTE: Settings under **Options** are available only when sessions are running in Classic User interface mode.

Window Title	Specifies the string that appears in the Reflection title bar. This string is also displayed on the taskbar when Reflection is running. If Reflection is running but minimized, the configured string is shown on the taskbar.

Enter up to 260 characters in the box. As you type in predefined shortcuts, options are added to the box. The predefined shortcuts and options are:

Shortcut	Option
&a	The Local IP Address
&c	Connected or No Connection
&d	Date (In the format set by Windows)
&f	Settings File Name or 'Untitled'
&h	Host Name
&n	Full Product Name
&r	Reflection
&s	Session Name
&t	Transport Type (Port Name)
&u	Product Name
&v	Product Version Number
&y	Terminal Type
&&	Ampersand Symbol (To produce one & symbol)

For example, if you set the Caption to &r - &s - &c, text similar to "Reflection Workspace - *hostname* via TELNET - Connected" is displayed in the Reflection title bar or on the taskbar, assuming Reflection is running but not minimized. (The exact text depends on your configuration.) The default for newly created sessions is &f - &n.

NOTE: Settings files from legacy Reflection display in Classic mode. Unsupported shortcuts from previous versions of Reflection settings files will be preserved and displayed as literal.

Show Menu Bar   Display the menu and toolbar in Classic mode.

NOTE: When this option is unselected, you can display the menu by clicking the Reflection button and then choosing **Show Menu Bar**.

Show Status Bar   Display the status bar in Classic mode.

Set Up Safeguards Dialog Box

Getting there

1 Open a VT terminal session.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click .
TouchUx	Tap the Gear icon and then select **Document Settings**.

2 Under **Terminal Configuration**, click **Set Up Safeguards**.

Safeguards

Clear display and scrollback buffer when disconnected	Delete all data from display memory when a session is disconnected from the host.
Save Secure Shell user name	Clear this option to prevent the user name you provide for this host session from being saved into the settings file, or recorded in a macro.
Cache Secure Shell user name	Select to temporarily store the user name entered for a Secure Shell session until the Reflection workspace is closed. (When this option is selected, users are not prompted for a user name when they reconnect unless they reopen the workspace. When it is unselected, the user name is cleared from memory immediately after a successful connection and users are prompted for a user name when they reconnect.)

Related Topics

- "Set Up Display Settings Dialog Box" on page 381

Connect to Host Dialog Box

This dialog box appears when you start a session for which no host has been specified.

The options are:

Host name	Type the host name or IP address of the terminal to which you want to connect.
OK	Click to connect the session immediately.
Cancel	Click to configure more than just the host name for this session.
	On the Quick Access Toolbar at the top of the workspace, click ![icon]. Then, under **Host connection**, click **Configure Connection settings**.

Reflection for HP

Reflection for HP is included with some Reflection products. It is not included in a default installation.

Installing and Configuring Reflection for HP

Installing Reflection for HP

To create and use HP terminal session, you need to install Reflection for HP. This feature is not installed by default.

- In the Reflection installer tree, expand **Workspace** > **Emulation** and install the feature called **HP with NS/VT**.

Starting HP Terminal Sessions

Reflection for HP is a separate application and runs in its own window. You can launch it from either the Start menu or from the Reflection Workspace.

To launch Reflection for HP do any of the following

- From the Workspace, open the **Create New Document** dialog box, and click **HP terminal**. (You must install the Reflection for HP feature to see this option.)

   -OR-

- From the Windows Start menu (or Apps list), go to **Micro Focus Reflection** > select **Reflection HP**.

   -OR-

- Double-click a Reflection for HP settings file (*.r1w).

Reflection for HP Settings Files

Although Reflection for HP now installs as part of Reflection Desktop, it continues to use the same settings files (*.r1w) and Visual Basic macros as in prior releases. If you are upgrading from an earlier version, you don not need to make any changes to your current settings.

Note that some security settings are shared by Reflection for HP, the Reflection Workspace, and the FTP Client. These include: Secure Shell settings and Reflection Certificate Manager settings.

For Additional Information about Reflection HP

Please send requests for help on undocumented features using the comment icon on this page. We will make an effort to respond to each of these queries individually and to add additional content to the documentation based on these requests.

NOTE: Commenting is available if you are viewing help from the Micro Focus website (the default). If you are viewing locally installed help, no comment icon is present; in this case, please contact Micro Focus technical support.

File Menu (Reflection HP)

The following options are available from the Reflection for HP File menu.

Export and Transform XML (Reflection HP)

HP Terminal > File > Import and Export

You can export and import Reflection for HP content using XML, including Reflection settings, data in the terminal window, and data in display memory. You can also use available options to transform this raw XML data into formatted data in the file type of your choice. As an example, you could specify that data in Reflection's terminal window be transformed to a text file. This would mean choosing the "Transform terminal screen to text.xsl" option.

The Export and Transform XML dialog box includes the following options:

Source XML	Specify which type of Reflection data should be the source for the XML to be generated.
Transform	Select **Transform** to translate the source using the stylesheet of your choice. Use the Browse button to view available transforms. Select **Export** only to save the source settings into an xml file whose name you type into the **Results file** box
Arguments	Use this option to supply parameters to transform files that accept or require arguments (Filter exported Reflection XML Settings.xsl and Transform mappings to text.xsl).

Layout Files (Reflection HP)

HP Terminal > File > Layout

You can use Reflection for HP layout files to save and open multiple Reflection for HP sessions. A layout file includes all the Reflection for HP sessions you have open when you save the layout. You can open the layout file when want to return to that configuration.

NOTE

- Reflection for HP sessions are not included when you save a layout from the Reflection Workspace.
- You can change a settings file after you create a layout. However, the window position, state, and size of the changed file are overridden by the layout file's last saved information.
- Deleted or moved settings files that are part of a layout file will cause the layout file to display an error message and open an untitled session in lieu of the displaced file.

Logging Settings (Reflection HP)

HP Terminal > File > Logging

Use this dialog box to configure logging and to enable serial device-to-host communications.

Logging copies data from display memory to the printer each time a linefeed is received so that attributes, such as underline, are printed. Normally logging is enabled by the host. However, if you want to configure a user-initiated logging session, select the Logging on check box.

Logging serves two different functions in Reflection:

- ◆ To provide user-initiated logging of your terminal session.
- ◆ To accommodate host printing, where an application turns on logging and starts sending data to either a printer or a file.

Difference between logging and printing:

- ◆ Logging parallels terminal-host printing.
- ◆ In logging, the host controls printing, bypassing Reflection. The Windows printer driver is still used, unless you enable **Bypass Windows print driver** in the **Print Setup** dialog box.

Serial Device-to-Host Communications	Reflection supports serial device-to-host communications (also called printer-to-host or printer 2-way communications). You can enable serial device-to-host communications when you want a device on a serial port (such as a printer or bar code reader) to be able to send information to a host via Reflection.
Logging On Check Box	Logging is usually enabled by the host. Select **Logging on** if you want to configure a user-initiated logging session.
Log Output to Serial Device	Select **Serial device** if you want a device on a serial port (such as a printer or bar code reader) to be able to send information to a host via Reflection. Selecting this check box enables VT terminal serial device-to-host communications.

Print (Reflection HP)

HP Terminal > File > Print

The printer selected in Print Setup is shown at the top of this dialog box (this could be the Windows default printer, another specific printer, or a disk file).

- ◆ **Display memory** prints the information visible on the display and information that has scrolled off of the display and is still in memory.
- ◆ **Screen** prints whatever you see in the terminal window.
- ◆ **Selection** prints any section that is highlighted in the terminal window.

Print Setup (Reflection HP)

HP Terminal > File > Print Setup

Use the Print Setup dialog box to control printer settings that apply only to Reflection for HP.

Bypass Windows Print Driver	By selecting this check box, you can send raw data (including printer control escape codes) directly to your printer. Output is sent to the printer immediately, instead of waiting for a whole page of information, and the Windows printing interface is bypassed.
	If you're bypassing Windows printing to a PostScript printer, the results may not be what you expect. PostScript printers are controlled by PostScript commands, which are typically sent to the printer from a PostScript printer driver. When you bypass this driver, one of two things will happen:
	◆ Some printers have built-in PostScript codes that are used when no driver can be found; so your output prints in the font determined by the printer's defaults.
	◆ If your printer depends on the driver for PostScript codes, then nothing (not even a blank page) will be printed when you select this check box.
Disable Printer Translation	This check box appears dimmed unless **Bypass Windows print driver** is selected.
	Select **Disable printer translation** to disable any character translation and to print characters exactly as they come from the host—no character set translation is made from the host character set to the PC character set. You should disable character translation if the host already generates characters in the correct character set for your printer, and your printer is not configured for the default IBM PC code page 437 character set.
	The **Disable printer translation** check box has little, if any, effect on screen printing or logging. When Reflection receives characters from the host, it automatically converts these characters to the ANSI character set before displaying them in Windows.

Page Options (Reflection HP)

HP Terminal > File > Page Setup > Page Options

Columns per Row	Enter a value from 10 to 999 (or select one of the standard options, 80 or 132). The printer columns automatically change when you change the number of **Columns** (on the **Screen** tab of the **Display Setup** dialog box).
Fit Font to Page	This check box is unavailable when **Use printer default font** is selected.
	When **Fit font to page** s cleared, printed fonts will always be correctly proportioned, but the text may not fill the printed page. When this check box is selected, Reflection adjusts the font's height and width, so that text always fills the printed page.
Auto Row Sizing	When this check box is selected, Reflection prints the optimal number of rows that can fit onto a page, given the parameters you specified in the **Page Setup** and **Page Options** dialog boxes for **Paper**, **Orientation**, **Text format**, **Column dimensions**, and **Row dimensions**.
	When the **Auto row sizing** check box is cleared, Reflection prints the number of rows per page specified in the **Rows per page** box.

Send Email (Reflection HP)

HP Terminal > File > Send

Send an email including any of the following:

- **Display memory** sends all text in display memory.
- **Screen** sends only the text shown on the terminal window.
- **Selection** sends the currently selected text.

Connection Menu (Reflection HP)

The following options are available from the Reflection for HP Connection menu.

- "Connection Setup (Reflection HP)" on page 391
- "More Settings – VT-MGR (Reflection HP)" on page 392
- "Connect Macro (Reflection HP)" on page 392

Connection Setup (Reflection HP)

HP Terminal > Connection > Connection Setup

The options available depend on which connection type you select.

Best network	Reflection for HP automatically selects which network protocol to use when connecting to a host. Reflection will first attempt to connect using Telnet, and then VT-MGR. Once Reflection has connected using a Best network protocol, it will make subsequent connections using the same protocol.
Telnet	Uses unsecured Telnet by default. Click Security to configure SSL/TLS or a Socks or HTTP Proxy.
VT-MGR	The VT-MGR connection type provides Network Services/Virtual Terminal (NS/VT) access to an HP 3000. "Fast file transfer" to an HP 3000 is automatically invoked when using Reflection for HP with NS/VT.
Secure Shell	Configure connections to a Secure Shell server. Secure Shell settings are shared with Workspace sessions.
	SSH config scheme is optional. If you leave this blank, changes you make to your Secure Shell settings are saved to Secure Shell configuration file under the current host name, and the settings you configure are applied by default to all Secure Shell connections to this host. If you specify a scheme name, changes you make to your Secure Shell settings are saved to the Secure Shell configuration file under the specified scheme name, and the settings you configure are applied to subsequent connections whenever you specify this scheme name.
Connect Macro	Specify a macro that will be executed when a settings file is loaded and a connection attempt is made.

More Settings – VT-MGR (Reflection HP)

HP Terminal > Connection > Connection Setup > VT-MGR > More Settings

Parity	This setting determines whether a parity bit is generated for each character transmitted. Parity is used to detect errors in data transmission; the number preceding the slash indicates the number of data bits sent.
	To use the multinational character set or 8-bit controls, **Parity** must be set to one of the values that offers 8-bit controls. If your communications link generates parity, and you set **Parity** to **8/None**, multinational characters appear on your screen. In this case, set **Parity** to either **8/Even** or **8/Odd**.
Optimize Ctrl Y	Optimizes Reflection to reduce its response time when receiving a Ctrl + Y (Set Break Request).

Connect Macro (Reflection HP)

HP Terminal > Connection > Connection Setup > Connect Macro

Macro Data	You can pass information to a macro by entering text in the **Macro data** box. Use the MacroData property within a macro to return this information.

Setup Menu (Reflection HP)

The following options are available from the Reflection for HP Setup menu.

- "Terminal Type (Reflection HP)" on page 393
- "Terminal Setup - Emulation Tab (Reflection HP)" on page 393
- "Advanced HP Options (Reflection HP)" on page 393
- "Terminal Setup - Keyboard & Mouse (Reflection HP)" on page 396
- "Terminal Setup - Margins Tabs (Reflection HP)" on page 397
- "Terminal Setup - Function Keys (Reflection HP)" on page 397
- "Display Setup - Colors (Reflection HP)" on page 398
- "Display Setup - Fonts (Reflection HP)" on page 398
- "Display Setup - Screen (Reflection HP)" on page 399
- "Display Setup - Options (Reflection HP)" on page 399
- "Event Setup (Reflection HP)" on page 400
- "Hotspot Setup - Settings (Reflection HP)" on page 400
- "Hotspot Setup - Defined Hotspots (Reflection HP)" on page 400
- "Keyboard Map Setup (Reflection HP)" on page 400
- "Mouse Setup (Reflection HP)" on page 401
- "Safeguards (Reflection HP)" on page 401
- "Toolbar Setup (Reflection HP)" on page 402
- "View Settings (Reflection HP)" on page 402

Terminal Type (Reflection HP)

HP Terminal > Setup > Terminal > Terminal type

The **Terminal Type** tab lets you specify which terminal you want Reflection for HP to emulate. You can configure Reflection for HP to emulate either an HP or a VT terminal.

When you pick a VT terminal, Num Lock is enabled, the display is cleared, and the cursor is positioned in the upper- left corner of the terminal window. Switching to a VT terminal type also changes the keyboard in the **Keyboard Map Setup** dialog box and the keyboard shown when you click the **Terminal keyboard** check box on the **Options** tab in the **Display Setup** dialog box.

NOTE: Changing the **Terminal type** value resets the values on all of the tabs on the **Terminal Setup** dialog box

---

Terminal Setup - Emulation Tab (Reflection HP)

HP Terminal > Setup > Terminal > Emulation

Use the **Emulation** tab options to set values specific to the type of terminal you are emulating (as indicated on the **Terminal Type** tab in this dialog box).

Online	Select to have Reflection for HP function as a terminal (also called "remote mode").
	Clear this option to enter local mode. In local mode, Reflection for HP does not attempt to communicate with a host computer. Characters entered from the keyboard appear on the screen, but are not transmitted to the host; nor is any data received from the host (for example, notification of a mail message).
	This value is not saved with your session settings.
Inhibit EOL wrap	When this check box is left cleared, Reflection automatically returns the cursor to the left margin in the next line when the cursor reaches either the right margin or the right screen edge. When selected, each one overwrites the character at the right margin until you explicitly move the cursor by pressing Return or using an arrow key.

Advanced HP Options (Reflection HP)

HP Terminal > Setup > Terminal > Emulation > Advanced

National Replacement Set	Some host systems use national replacement characters to encode characters that are not available in the ASCII 7-bit character set. If necessary, set this list to match the set used by your host. In 8-bit operation, the value in this list has no effect. In 7-bit operation, however, the value assigned here limits characters to those that are defined for the configured set, and determines the replacement characters that are used during data communications.
Field Separator	When Reflection is transmitting in block, page, and format modes, it sends a field separator character after each field of the formatted screen except the last one.

Block Terminator   Under certain conditions, Reflection transmits a block terminator character at the end of each block of data transmitted. The value selected here specifies which ASCII character is sent to indicate that the end of the block has been reached.

Return Definition   From these two lists, select a string of one or two characters to be generated whenever Return is pressed. If the second character is a space, only the first character is generated.

Host Prompt   An HP 3000 sends a DC1 character to indicate to Reflection that it is ready to accept a line or block of characters. This character is sent immediately after the MPE prompt is sent. This list allows you to change which character is expected.

Most hosts either use the DC1 (^Q) character or no prompt (that shows up simply as a space). Select the appropriate host prompt from this list. (Press Alt+M then select DISPLAY FUNCTIONS to see the control codes sent by the host.) When Typeahead is selected (Terminal Setup > Keyboard & Mouse), Reflection waits for this prompt to be received from the host before it transmits the next line from the keyboard buffer.

Start Column   For every line in display memory, Reflection attempts to remember the leftmost column that was entered from the keyboard, as opposed to that received from datacomm. This way, Reflection can distinguish the host prompt portion of each line from the user-entered portion. This information is used when you enable LINE MODIFY or MODIFY ALL to determine the leftmost column that should be transmitted to the host when you press Enter or Return.

Under some circumstances, it is impossible for Reflection to tell which column was the first user-keyed column; when that happens, it uses the value you enter in this box to determine the leftmost column to be transmitted. When your display Columns are set to 80, enter a value from 0 to 79. When you're in 132-column mode, enter a value from 0 to 131.

Forms Buffer Size   This box is active only when the Terminal type list on the Emulation tab is set to HP70094, HP70098.

NOTE: It is recommended that you not change this value; it's best left set by the host using escape sequences.

This value specifies the amount of memory (in 256-byte blocks) to be allocated to the forms cache buffer. If you change the buffer size, the contents of display memory and the printer buffer are cleared. If there is not enough memory to increase the forms buffer to the specified size, its size is not changed.

Transmit   This list box is active only when Terminal type on the Emulation tab is set to HP70094, HP70098.

The value here determines whether Reflection transmits all fields in format mode (All) or only those fields that have been modified (Modified). This value is typically set by the host application.

Use Host Prompt	Clear this check box if you want Reflection to ignore the host prompt; the value in the **Host Prompt** list clears. Conversely, when you select any value from the Host prompt list other than null (^@), the **Use host prompt** check box is selected.
	Clearing the **Use host prompt** check box has the same effect as selecting the I**nhibit Handshake** and **Inhibit DC2** check boxes. Ignoring the host prompt forces Reflection to behave as though both inhibits are on, thus preventing handshaking. Over an X.25 network, this prevents communications problems caused by applications that use handshaking.
	When the **Use host prompt** check box is cleared, Reflection always responds to a primary status request from the host that both **Inhibit handshake** and **Inhibit DC2** are enabled. This can affect a host application that explicitly changes one of these inhibits.
Inhibit Handshake	This check box, along with **Inhibit DC2** and some other factors, determines the type of handshaking that precedes each block transfer of data from Reflection to the host system. When selected, the DC1 handshake for block transfers is inhibited.
Inhibit DC2	This check box, along with **Inhibit handshake** and some other factors, determines the type of handshaking that precedes each block transfer of data from Reflection to the host system. When selected, the DC2 handshake for block transfers is inhibited.
	Most of the keys on the keyboard have an associated ASCII character. Several keys, however, perform functions for which there is no character defined; for example, Home and PgUp. Certain host software programs, such as HP Slate, need to be informed when you press one of these non-ASCII keys. Selecting this option signals Reflection to inform the host system whenever you press one of these keys
	.When this check box is selected and Reflection is operating in character/remote mode, each time you press one of these keys the associated escape sequence is transmitted to the host.
	Num Lock: Alt+J (clear display)
	Scroll Lock: Alt+K (clear line)
	Home: Alt+D (delete line)
	UpArrow: Alt+I (insert line)
	PageUp: Alt+Y (command window)
	LeftArrow: Ctrl+End
	RIghtArrow: Ctrl+UpArrow
	End: Ctrl+DownArrow
	DownArrow: Ctrl+LeftArrow
	PageDown: Ctrl+RightArrow
	Insert: Ctrl+PageUp
	Delete: Ctrl+PageDown
	Caps Lock: Ctrl+Home
	Most applications that require this feature automatically send the escape sequences to enable and disable the feature, so you probably will never need to enable it manually.

SPOW	Ordinarily, the Spacebar overwrites and erases existing characters. When the SPOW (SPace OverWrite) check box is selected, spaces entered from the keyboard (not spaces echoed from the host), move the cursor over existing characters, but do not overwrite them with spaces:

  - The SPOW latch is turned on by a carriage return.
  - The SPOW latch is turned off by a linefeed, tab, or home up.

Format Mode	Format mode is a mode of terminal operation in which the display is made up of protected and unprotected fields. When this check box is selected, data can only be entered in unprotected fields.
Block Transfer Unit	If Reflection is operating in block mode, a block of one or more characters is transmitted when you press Enter or when the host requests a block transfer from terminal memory. This option determines how much data Reflection transmits on each block transfer. When set to Line, data is transmitted one line at a time, or one field at a time in format mode. When set to Page, data is transmitted one page at a time.

Terminal Setup - Keyboard & Mouse (Reflection HP)

HP Terminal > Setup > Terminal > Keyboard & Mouse

The **Keyboard and Mouse** tab lets you select keyboard options, such as typeahead and destructive backspace, and the function of VT terminal keys if you have a VT terminal selected as your Terminal type. You can also use the **Standard File and Edit menu shortcuts** option to cut and paste. This supports standard Windows cut and paste keyboard shortcuts.

Destructive Backspace	By default, pressing Backspace moves the cursor to the left without erasing characters. Select this check box to erase the character to the left of the cursor when you press Backspace.
Typeahead	With an HP 3000 in character mode and remote mode, you must wait for a host prompt before entering new data. After the host has processed your input, it transmits a prompt to Reflection for HP as a signal to start sending more data. The host ignores any characters it has received before sending its prompt.

By selecting the **Typeahead** check box, you can type continuously without waiting for the host prompt; Reflection stores your keystrokes in a buffer until the host prompt arrives. When it does, Reflection sends the next line of keyboard input from its buffer. The keyboard never locks when **Typeahead** is enabled, so if you know what you must type next, you can go ahead and type it.

To see what the prompt character is set to, look at the **Host prompt** list in the Advanced HP Options dialog box (from the Emulation tab); the default is ^Q (DC1).

To clear the buffer, click **Reset-Clear Typeahead** on the Connection menu.

When **Typeahead** is enabled, it is sometimes necessary to clear Reflection's typeahead buffer. Click Reset-Clear Typeahead on the Connection menu to clear Reflection's typeahead buffer.

Caps Lock Mode	Select this check box to limit the characters produced from the keyboard to 37 Teletype-compatible codes:

- No lowercase alphabetic characters are generated. All alphabetic keys appear as if they are shifted.
- The ~ (tilde) and ` (grave accent) are disabled.
- The characters {, |, and } are converted to the characters [, \, and].

Return = Enter	The HP enter function is mapped by default to the Enter key on the numeric keypad. If you prefer to use Return for the HP enter function in block mode applications, select this check box. Selecting this check box may cause problems if your host system expects a carriage return.
Asian Keyboard Interpreter	This item appears dimmed in VT mode. It also appears dimmed in HP mode if you do not have a double-byte character set selected in the **Host character set** list on the Emulation tab.

When connecting to an HP 3000, selecting this check box makes the terminal screen cursor actions consistent between single-byte and double-byte characters. For example, on a terminal screen with mixed single- and double-byte characters, pressing the Backspace key once moves the cursor through one double-byte character or one single-byte character. When this check box is cleared, it's necessary to press the Backspace key twice to move through a double-byte character and once to move the cursor through a single-byte character.

This check box should typically be checked when connecting to an HP 3000. This check box should be cleared when connecting to an HP 9000 or a UNIX host because double-byte translation is handled by the host.

Terminal Setup - Margins Tabs (Reflection HP)

HP Terminal > Setup > Terminal > Margins Tabs

The Margins Tabs tab lets you set left and right margins and tab stops in Reflection for HP.

Terminal Setup - Function Keys (Reflection HP)

HP Terminal > Setup > Terminal > Function Keys

The **Function Keys** tab lets you select which set of key labels are displayed along the bottom of your screen, and lets you customize eight user keys. A user key definition consists of the following:

- A 16-character label (eight characters per line)
- A string of up to 80 characters that is produced when the key is pressed
- An attribute determining how Reflection processes the string when the key is pressed

Function Key Set	This option determines which set of function key labels display at the bottom of the terminal window.
Insert Special Characters	To include escape sequences and ASCII control codes in the user key string, select **Insert special characters**. If you're using the Tab key to tab through the dialog box fields, you must clear the **Insert special characters** check box; otherwise you'll insert the ASCII tab character each time you press the Tab key.
	The following list shows some examples of keys and key combinations that create certain escape sequences (shown by the two-letter mnemonic that appears on your screen):
	Enter : CR
	Tab : HT
	Backspace: BS
	Esc : EC
	Ctrl+Q: D1
	Ctrl+S: D3
	Ctrl+E : EQ
	Ctrl+X : CN

Display Setup - Colors (Reflection HP)

HP Terminal > Setup > Display > Colors

Use the Colors tab to customize your screen color and different host attributes (such as inverse blinking text). For each item, you can select text attribute colors and background colors. For plain text, the background sets the color for the Reflection for HP terminal window. Once you've created a set of colors you like, you can save the color partial settings file to a partial settings file that contains only color information.

Display Setup - Fonts (Reflection HP)

HP Terminal > Setup > Display > Fonts

Use the Fonts tab in the Display Setup dialog box to customize your display font.

Auto Font Sizing	When **Auto font sizing** is selected, Reflection for HP will automatically resize the font to fit all text in the terminal window.
	NOTE: This option is greyed and cleared when **Dynamic terminal size** is selected in **Connection** > **Connection Setup** > **More Settings** for Secure Shell and RLogin connections.
Space Compensation	This option is used on systems running the Thailand edition of Windows. The value that you set here specifies the number of consecutive space characters that will trigger white space compensation when displaying a line containing Thai characters.

Display Setup - Screen (Reflection HP)

HP Terminal > Setup > Display > Screen

Set display options, such as the number of rows and columns, cursor type, scrolling attributes, and other display attributes.

Columns	Sets the width of the scrolling region in the terminal window. You can select 80 or 132; or use the spin box to specify any value between 80 and 999.
Memory Blocks (8K Each)	Display memory contains both the information visible on the display and information that has scrolled off of the display. This box sets the amount of memory you want to allocate to display memory. The default setting is for 9 blocks of 8 kilobytes each, or 72K of display memory.
	The number of bytes you are currently using is calculated on each character of text; you'll have more "pages" of display memory when your text lines do not run all the way out to the right margin.
	The default value holds approximately 22 pages of display memory when each line is exactly 80 characters long.
Scrolling	Smooth scrolling limits the speed at which new lines appear on the screen. Jump scrolling allows lines to be displayed as quickly as they are received from the host.

Display Setup - Options (Reflection HP)

HP Terminal > Setup > Display > Options

Window Title	Use this option to customize the name of your Reflection for HP window. You can enter text and/or any of the following special characters:

&a   The local IP address

&c   Connected or not connected

&d   Date (in the format set by Windows)

&f   Settings file name or "Untitled"

&h   Host name

&i   Instance number of Reflection for HP

&l   Layout file name

&n   Full product name

&r   Reflection

&s   Session name

&t   Transport type (port name)

&u   Product name

&v   Product version number

&y	Terminal type
&&	Ampersand (that is, use two && to produce one &)

Time Connected	Displays a time counter on the status bar that shows the time you have been connected in hours, minutes, and seconds (hh.mm.ss).
Slash Zeros	Specifies whether zeroes displayed in the terminal window contain slashes (like this: Ø). Selecting this option may make it easier to work with numeric data.

Event Setup (Reflection HP)

HP Terminal > Setup > Events

Use the Events Setup dialog box to create and manage events in Reflection for HP

Use predefined Reflection events to initiate Reflection actions, such as Reflection for HP macros, and menu and terminal commands when an event is encountered during a host session. This allows you to monitor Reflection/host interactions and synchronize Reflection commands with a defined group of host session events.

Hotspot Setup - Settings (Reflection HP)

HP Terminal > Setup > Hotspots

Hotspots are buttons that appear over common host commands in terminal sessions. Typically, clicking a hotspot transmits a terminal key or command to the host.

Use the **Settings** tab to configure the mouse click that activates hotspots and whether to enable or show hotspots.

Hotspot Setup - Defined Hotspots (Reflection HP)

HP Terminal > Setup > Hotspots > Defined Hotspots

Use the **Defined Hotspots** tab to configure where hotspots will appear in the terminal screen and what actions occur when the user clicks each hotspot.

By default, Reflection for HP defines hotspots for most common terminal commands.

Keyboard Map Setup (Reflection HP)

HP Terminal > Setup > Keyboard Map

The Keyboard Map Setup dialog box lets you substitute a simple keystroke for complex and repetitive keystrokes or mouse actions. When you map a keystroke to a terminal function, string, macro, menu or terminal command, that key becomes a keystroke for the specified action.

To find a keystroke's current mapping

◆ Under **PC keyboard**, click a mapped cyan/teal key and note the corresponding **Action** in the lower half of the dialog box.

To map a keystroke

1 Under **PC keyboard**, select the PC key or keystrokes that will execute the action.

2 Select and configure an **Action**.

3 Click **Map**.

Mouse Setup (Reflection HP)

HP Terminal > Setup > Mouse Map

To map a mouse event to an action

1 Configure the mouse action in the top of the dialog box.

2 Select and configure an **Action**.

3 Click **Map**.

Safeguards (Reflection HP)

HP Terminal > Setup > Safeguards

Host name	Use this option to control whether host names will be saved with your host connections or connect macros. By default, the host name you provide for this host session is saved in the settings file. Clear this check box to prevent the host name from being saved into the settings file or recorded in a macro.
Passwords (using weak encryption)	Use this option to control whether passwords should be saved with host connections or in connect macros. Saving a password in a recorded script means the password is encoded and not visible when a macro is examined. The preferred solution is to use Secure Shell public keys.
	When this setting is changed it takes effect only for new macros and does not automatically update pre-existing Reflection for HP macros. To update a macro, re-record it with the Passwords option set to the value you wish saved in the macro.
	NOTE: It is not possible to manually edit the password value in a macro and retain the encrypted state.
Clear display and scrollback buffer	Use this option to have Reflection delete all data from display memory when a session is disconnected from the host.
Clear Clipboard	Use this option to delete all data from Windows Clipboard when exiting Reflection.
	NOTE: Reflection will remove data from the Clipboard even where the data was saved from a different application.

Toolbar Setup (Reflection HP)

HP Terminal > Setup > Toolbar

The Toolbar Setup dialog box contains the following tabs:

Toolbars

View predefined toolbars and descriptions of the buttons on the selected toolbar. You can use this tab to create, rename, delete, and hide or display a toolbar, or reset it to its factory defaults.

Predefined buttons

Add buttons to the toolbar from the library of predefined buttons. Select a category on this tab to see the available buttons.

Customize

Add a picture to a button or create new buttons that launch a Reflection for HP macro; execute Reflection for HP menu, terminal, or Visual Basic commands; or send text to a host.

Settings

Set the location of the toolbar and change its appearance.

View Settings (Reflection HP)

HP Terminal > Setup > View Settings

The **View Settings** dialog box enables you to view and change all Reflection for HP settings from a single location. Use the **Search** box to locate settings using all or part of the setting name.

You can use this dialog box to check the current value of a setting, change a settings value, and to find out what valid values are for each setting. When you change a setting here, the corresponding setting in a dialog box changes, too (if there is one).

Use the **Advanced** button to filter setting information to view mapping-only settings, enabled and disabled settings, or settings that are saved in Windows registry.

You can view the settings in descriptive or programmatic formats by selecting either **Descriptive text** or **Macro syntax** respectively.

NOTE: You can find detailed information about individual settings using the Reflection for HP programming reference. Select **Macro syntax** to determine the programmatic name for the setting, then search for that name in the programming guide available here: http://docs.attachmate.com/reflection/14.x/prog-ref/hp-unix-openvms/.

Macro Menu (Reflection HP)

Reflection for HP supports Visual Basic for Applications macros as well as two older programming languages (Reflection Basic and RCL). It does not support the .NET API.

You can create macros using the macro recorder or by using the Visual Basic Editor. Once you have created macros, you can run them using the **Macros** command on the **Macro** menu, or you can configure events, hotspots, mouse clicks, or toolbar buttons to run macros.

- "Macros Dialog Box (Reflection HP)" on page 403
- "Recording Macros (Reflection HP)" on page 404

Macros Dialog Box (Reflection HP)

HP Terminal > Macro > Macros

Reflection for HP provides macro support using Visual Basic. When you record macros in Reflection or create new macros using the **Create** button in the **Macros** dialog box, they are placed in a module called NewMacros. Macros are saved in your Reflection for HP settings file (*.r1w).

In writing and editing Reflection macros using Visual Basic projects you will be working with:

- Visual Basic features that are common to all Visual Basic applications. These features include the Visual Basic Editor, Basic language programming commands that are common to all Visual Basic implementations.
- Methods, properties and events that are specific to Reflection for HP sessions and allow you to configure and manipulate these sessions.

Context-sensitive help from the Visual Basic Editor for Reflection for HP commands is provided by an installed Windows Help file. On newer Windows system, support for viewing Windows help (*.hlp) is no longer available by default. See Knowledge Base Article 7021283 (https://support.microfocus.com/kb/doc.php?id=7021283) for information about how to configure this support.

The Reflection for HP Programming Reference information is also available on the support website here: http://docs.attachmate.com/reflection/14.x/prog-ref/hp-unix-openvms/.

Macro data	Use this field to pass information to the macro. Within a macro, use the **MacroData** property to access this value.
Export	Export the selected macro to a macro file.

Macro Files

Macro files are plain text files that provide a way to save simple macros independently of Reflection for HP settings files (*.r1w). Each macro file contains exactly one macro. Macros are limited to a single subroutine; and cannot call other routines or user forms.

Any recorded macro will run successfully as a macro file because all the code in any recorded macro is contained within a single subroutine. However, if you have created another macro (MacroB) that includes a call to your recorded macro (MacroA), MacroB will not run correctly after being exported to a macro file because the code in MacroA is not included in the exported file.

You can create a macro file when you save a recorded macro by setting **Destination** to **Macro File**. You can export an existing macro to a macro file using the Macros dialog box **Export** option.

Related Topics

◆ "Macro Menu (Reflection HP)" on page 403

Recording Macros (Reflection HP)

HP Terminal > Macros > Connection Setup > Start Recording | Stop Recording

The macro recorder allows you to capture actions you perform in Reflection for HP. For example, to create a login macro, you can turn on the macro recorder, log on to a host, then stop recording.

Stop Recording Dialog Box Options

Destination	You can save recorded commands as a Visual Basic Macro, a Macro File, or as text to the Clipboard.
	When you select **Macro** (the default), the recorded macro is not saved until you save your Reflection for HP settings.
Create a button	Creates a new toolbar button that will run the macro you are recording.
Make this the connect macro	Connect macros run immediately after Reflection has successfully made a connection to the host. The name of the connect macro for a Reflection for HP session can be viewed and edited from the Connection Setup dialog box.

6530 Sessions

To connect to NonStop (Tandem) hosts using the NonStop standard 6530 emulation type, you'll need to purchase and install the Reflection Desktop for NonStop Add-On. This add-on allows you to use any program built for the Guardian operating system. This section shows you how to configure Reflection for NonStop to connect to your host, and how to alter any other relevant settings.

◆ "Configure Connection Settings Dialog Box (6530)" on page 405
◆ "Configure Advanced Connection Settings Dialog Box (6530)" on page 406
◆ "Set up Connection Security (6530)" on page 408
◆ "Configure SSL/TLS Security (6530)" on page 409
◆ "Configure SSH Security(6530)" on page 410
◆ "Configure Terminal Settings (6530)" on page 412
◆ "Set Up Display Settings (6530)" on page 414
◆ "Configure Recent Typing (6530)" on page 416

NOTE: For information about creating and editing macros, using file transfer, logging, and other features, see the 6530 Help available on the Session ribbon Help group.

Configure Connection Settings Dialog Box (6530)

Getting there

1 Open a 6530 terminal session.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ⬚.
TouchUx	Tap the Gear icon and then select ⬚ **Document Settings**.

2 Under **Host Connection**, click **Configure Connection Settings**.

From this dialog box, you can specify the settings for a 6530 connection.

NOTE: For information about creating and editing macros, using file transfer, logging, and other features, see the 6530 Help available on the Session ribbon Help group.

Connection

Host name/ IP address	Enter the host name of IP address of the host you want to connect to.
Port	Enter the port number that the Telnet server listens on here. The default is the "well known" telnet port number 23.
Service (or Window name)	Optionally enter the service name (i.e. TACL or any other service that has been defined on this telnet server), or the name of a window that has been defined on this telnet server.

Host Connection Options

Use Line Mode	If checked, line mode is used. Unselect if you want to run in character mode. Line mode should always be used for connections to Guardian sessions on a NonStop host.
Automatically connect to the host	If checked, the session connects to the host as soon as it is opened.
Automatically reconnect when connection is lost	If checked, and the session is lost for any reason, the session automatically reconnects.

Alternate/Backup hosts

Use this section to configure for alternate hosts, which is a form of load balancing (i.e. if an application is running on several hosts and there are many users, load balancing is accomplished by randomly connecting to one of the hosts in the list of available hosts), or for backup hosts, which provides a backup host in the event the first host doesn't respond.

Disable Alternate/Backup Hosts	If this item is selected, connections go to the IP address specified in the **Connection** section above.
Enable Alternate Hosts (Load Balancing)	If this item is selected, alternate hosts are used and fields are displayed for entering host names and ports.
	The order of alternate hosts is not relevant, because the host is selected randomly.
Enable Backup Hosts	If this item is selected, backup hosts are used and fields are displayed for entering host names and ports.
	To change the order of backup hosts, use the **Move Up** and **Move Down** buttons.

Configure Advanced Connection Settings Dialog Box (6530)

Getting there

1 Open a 6530 terminal session.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click .
TouchUx	Tap the Gear icon and then select **Document Settings**.

2 Under **Host Connection**, click **Configure Advanced Connection Settings**.

From this dialog box, you can specify the advanced settings for a 6530 connection.

NOTE: For information about creating and editing macros, using file transfer, logging, and other features, see the 6530 Help available on the Session ribbon Help group.

Connection Timers

Connection Timeout	This field is used to specify the maximum amount of time, in seconds, to wait for a connection to the remote host to complete. The default 10 seconds should be enough for almost any connection - however, if your connection fails and you are sure that the host you are trying to connect to is up, increase this value.
Reconnection Interval	This field is used to specify the amount of time, in seconds, to wait before another attempt to connect is made.

Connection Action

This section is used to select a macro to run before connecting, and/or a macro to run after the connection has completed. For details on creating, recording and editing macros, please see "Create and Edit Macro Files" in the 6530 Help available on the Session ribbon Help group.

Run a macro before the initial connection	If this item is checked, the **Select Macro...** button is active, allowing you to select a macro to run before the connection is attempted. **NOTE:** this macro only runs when the session is opened.
Run a macro after the initial connection	If this item is checked, the **Select Macro...** button is active, allowing you to select a macro to run after the connection has completed.
Run when reconnecting	If this item is checked, the macro defined to run after the initial connection also runs when re-connecting.

Miscellaneous

Send Keep Alive packets	Check this box if you want to enable Keep Alive messages. Keep Alive sends a packet to the host periodically to determine if the connection is still open. **NOTE:** You cannot set the duration between keep alive messages as that is an operating system issue.
Enable TCP/IP Trace	Select to trace all TCP/IP traffic for this session. This creates a trace file named TCPD.TRC in the configuration directory, which is normally: `Documents\Micro Focus\Reflection\HPNonStop\Logs`.
FTP Port	Use this item to set the port to use for FTP sessions using the built-in FTP client. For clear text sessions, this would normally be port 21.

Screen Size

Conversational Mode	This field is used to set the size of the screen in rows and columns while in conversational mode. You may select one of the common sizes from the pull down menu, or select **Custom Size** from the pull down and then select the size you prefer in the **Rows and Columns** boxes below this item. The minimum number of rows and columns is 24 and 80, and the maximum number of rows and columns is 54 and 150.
Block Mode	This field is used to set the number of rows and columns to use while in block mode. If set to the same value as conversational mode, then the display does not change when switching between modes. If set to a different value than conversational mode, then the display changes to the selected size when switching to block mode, and back to the conversational size when switching back to conversational mode. **NOTE:** Since many NonStop block mode applications only know 24x80, unless you are sure your application can use a different size it's best to leave this field at 24x80. The one known exception is "tedit", which will work at 24x80, 27x132, 48x80, and 54x132.

Set up Connection Security (6530)

Getting there

1 Open a 6530 terminal session.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click .
TouchUx	Tap the Gear icon and then select **Document Settings**.

2 Under **Host Connection**, click **Set Up Connection Security**.

This dialog is used to turn on one of the security (encryption) options.

NOTE: For information about creating and editing macros, using file transfer, logging, and other features, see the 6530 Help available on the Session ribbon Help group.

Security

Use SSL/TLS	If this item is checked, SSL/TLS is used for Authentication/Encryption and you can use the **Configure SSL/TLS** button to open the Configure SSL/TLS Security dialog box.
Use SSH	If this item is checked, SSH is used for Authentication/Encryption and you can use the **Configure SSH** button to open the Configure SSH Security dialog box.

Configure SSL/TLS Security (6530)

Getting there

1 Open a 6530 terminal session.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ![icon].
TouchUx	Tap the Gear icon and then select ![icon] **Document Settings**.

2 Under **Host Connection**, click **Configure SSL/TLS Security**.

This dialog box is used to configure a session for SSL/TLS security.

NOTE: For information about creating and editing macros, using file transfer, logging, and other features, see the 6530 Help available on the Session ribbon Help group.

Server Authentication

This item selects the type of server authentication to use for the connection. Note that you can select multiple types.

Check for valid CA signature	If checked, the SSL/TLS Certificate is checked to verify that it has a valid CA signature.
Certificate host name must match host being contacted	If checked, the host name specified in the certificate must match the host name you are connecting to.
Perform CRL check	If checked, the certificate is checked against a Certificate Revocation List, and if the certificate has been revoked, the connection will fail.

Client Certificate

If you require both host and client authentication, fill in this area.

Provide client certificate If checked, the client certificate specified in the **Client certificate file** box will be sent to the host.

Client certificate file Enter the client certificate filename and path, or click on the Browse button to start a file open dialog.

Client certificate file password If the client certificate file has a password, enter it here.

Secure File Transfer

This section is used to enable SSL/TLS (FTPS) for file transfers using the built-in FTP client.

Use FTPS Check this item if you want to use FTPS to secure FTP sessions using the built-in FTP client.

Port Enter the port number to use for FTPS sessions using the built-in FTP client.

SSL/TLS logging Select whether or not to do diagnostic logging of the session, and what level of logging should be done.

Leave the default (**None**) selected unless you have a problem with the connection.

The resulting log file, named SSLLog.log can be sent to support to help diagnose the problem. The log file is placed in the configuration directory, normally Documents\Micro Focus\Reflection\HPNonstop\Logs.

If **Negotiation Only Data** is selected the log file contains data related to the establishment of the session, and does not contain any sensitive data such as passwords.

If **Negotiation and Session Data** is selected the log file contains all data, including passwords. Since most SSL/TLS issues occur during negotiations this setting should only be selected if the session drops after negotiations are complete.

Configure SSH Security(6530)

Getting there

1 Open a 6530 terminal session.

The steps depend on your .

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ![icon].
TouchUx	Tap the Gear icon and then select ![icon] **Document Settings**.

2 Under **Host Connection**, click **Configure SSH Security**.

This dialog box is used to set up SSH connections to the NonStop host.

NOTE: For information about creating and editing macros, using file transfer, logging, and other features, see the 6530 Help available on the Session ribbon Help group.

SSH Configuration

This item selects the type of server authentication to use for the connection. Note that you can select multiple types.

Username	Use this field to specify the username on the SSH host. A username is required for all authentication methods.
User Authentication	This area is used to specify the type of authentication used when connecting to the SSH host. Valid choices are:
	Password: Use Username/Password only to authenticate.
	Public Key: Use keys only to authenticate.
	Keyboard Interactive: Use Keyboard Interactive (host prompts for Username/Password).
	GSSAPI: Use GSSAPI (Username/Passwordand/or keys are not required).
	If **Public Key** or **Password and Public Key** are selected, enter the private key path and file name, or click the Browse button to select it.
	If the private key file has a password, enter it in the Private key password field.
	NOTE: If the private key file has a password but it is not entered here, you will be prompted for it when you connect. The password is encrypted in the configuration file. For better security, it is suggested that this field be left blank so that the user must enter the password when connecting.
Encryption	Use this field to specify the encryption strength. Valid choices are:
	Auto Select: Let the software decide – picks strongest available
	DES: Use DES encryption
	Triple DES: Use triple DES encryption
	AES: Use AES encryption
	Blowfish: Use Blowfish encryption

Compression	Use this field to specify the compression level to use. The middle of the scale is a good combination of speed and compression. You can leave this set to **Auto Select** to have the software decide for you.
Banner window	If checked, the greeting message from the host will appear in a separate window instead of on the emulation screen.
Enable logging	If checked, the session is logged to SSHLog.log in the user configuration directory (normally Documents\Micro Focus\Reflection\HPNonStop\Logs). This field is normally left unchecked unless you have problems connecting or during a session, in which case you should turn logging on, reproduce the problem, and send the resulting log file to support to aid in diagnoses.
Port Forwarding	**Use port forwarding**: If this item is checked, the connection to the host is forwarded through the SSH server to the port specified in the Port field. **Port**: Enter the port to forward connections to.
Startup Options	**Default shell** If this option is selected, you will get the default UNIX shell on the system you are connecting to. **Execute command** If this option is selected, enter the command you wish to execute in the field below. The session will connect, run the command, and close the connection. **Run program** If this option is selected, enter the program to run in the field below. The session will connect, run the program, and when you exit the program, close the connection.
Inactivity Timeout	**Enable inactivity timeout**: If this item is left unchecked the inactivity timeout is disabled. Otherwise fill in the field below with the timeout specified in seconds.
Secure File Transfer	**Use SFTP** Check this item to enable secure file transfers via SSH (SFTP) when using the built-in FTP client.
Host Check	If set to No, all connections are accepted. If set to Yes and the host is not known, then the connection is refused. If set to Ask User, if the host is not yet known the user is prompted as to whether to accept the connection, and whether or not to trust this host in the future.

Configure Terminal Settings (6530)

Getting there

1 Open a 6530 terminal session.

The steps depend on your .

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ⬚.
TouchUx	Tap the Gear icon and then select ⬚ **Document Settings**.

2 Under **Terminal Configuration**, click **Configure Terminal Settings**.

This dialog box is used to configure 6530 terminal settings.

NOTE: For information about creating and editing macros, using file transfer, logging, and other features, see the 6530 Help available on the Session ribbon Help group.

Audio Alarm

Enable beep	If checked, anything that would cause a bell causes an audible alert. This includes receiving a bell character from the host, or a margin bell if it is enabled.
Enable bell column	If checked and Enable Beep is checked, the margin bell rings at the column specified in the Bell Column field.
Bell column	Enter the bell column number here.

Keyboard Options

Enable type ahead	This item specifies whether the emulator buffers keystrokes when the keyboard is locked, or when data is received from the NonStop.
Use enter key as a function key	This item specifies whether the Enter key is treated as an extra function key in block mode.
Enable PF key support	This item specifies whether or not the emulator supports PF keys. When PF key support is enabled (checked) pressing any function key transmits both the key press and the contents of modified fields on the display to the Host computer. When disabled (not checked), only the key press is transmitted.
Convert input to upper case	If checked, all input typed in at the keyboard is forced to upper case, regardless of the state of the shift or caps lock keys.

Identification

Terminal ID	This item specifies the character used to identify the exact terminal type being emulated. Programs on your Host computer can use this character to modify their behavior.
Firmware revision	This item specifies a three character string which identifies the firmware revision of the terminal being emulated. Some programs on your Host computer may refuse to run if they detect an old firmware revision, and this string can be used to prevent that from happening.

HLLAPI

Short name	This item specifies the HLLAPI short name of the session. Valid values are A to Z.
Long name	This item specifies the HLLAPI long name of the session.

Memory

Memory pages	This field defines the number of scroll back pages that are available for data that has scrolled off the screen. The default value should be 12, and the maximum value is 400.

Language

Language	This item specifies the national character set used for communications with the Host computer. Languages ending with 7 are 7-bit national character sets. Languages ending with 8 use the 8-bit ISO 8859-1 / Windows ANSI character set.
Host supports Euro symbol	Check this item if the host supports the Euro symbol.
Enable line drawing character substitution	Check this item to replace foreign characters with line drawing characters.

Hot Spots

Enable hot spots	This item turns hot spot processing on and off. If enabled (checked), control double mouse clicks behave differently in conversational and block modes as follows: **Conversational**: Control double clicking on a word places that word at the current cursor position, followed by a carriage return. For instance, at the telnet server "Enter Choice>" prompt you can control double click on one of the available services listed and it is sent to the cursor location followed by a carriage return. Words are delimited by any non-alpha or non-numeric character. Control double clicking on any function key labels (Fn or SFn (i.e. F1, F14, SF1, SF14)) sends that function key. **Block**: Control double clicking on any function key labels (Fn or SFn (i.e. F1, F14, SF1, SF14)) sends that function key.

Set Up Display Settings (6530)

Getting there

1 Open a 6530 terminal session.

   The steps depend on your .

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click .
TouchUx	Tap the Gear icon and then select **Document Settings**.

2 Under **Terminal Configuration**, click **Set Up Display Settings**.

This dialog box is used to configure display attributes, display speed, and other display settings.

NOTE: For information about creating and editing macros, using file transfer, logging, and other features, see the 6530 Help available on the Session ribbon Help group.

Display Attributes

Display underline	This item specifies whether the monochrome underline attribute is displayed.
Underline special	This item specifies how the underline attribute is displayed. If checked, the character location before an underline attribute field is a different color than the rest of the field. If unchecked, the character location before an underline input field is the same color as the rest of the field.
Allow invisible mapping	This item specifies how the invisible attribute is displayed. If checked, invisible attribute fields are visible and therefore can be used to display more colors on the screen. If unchecked, invisible attribute fields are invisible.
Display blinking text	If checked, fields marked as blinking by the host will blink.
Blink rate	Select the speed at which the blink occurs.

Display Speed

Display delay	This item specifies the delay period between receipt of characters and updating of the display. The higher the value is, the longer the delay. For the Telnet access method this is best left at 1.
Scrolling speed	This item specifies how many lines of data the 6530 emulation will receive before forcing the on-screen display to be updated when it is receiving large amounts of data. Higher values result in faster scrolling.

Color Control

Allow host color changes	This item specifies whether the 6530 emulation changes the color map when the host sends color change escape sequences. Uncheck this item if you prefer your own color mapping.

Scroll Bar

Display Vertical Scroll Bar	If this item is checked a vertical scroll bar appears on the right side of the emulation screen, allowing you to move through display memory. **NOTE:** This is effective in Conversational mode only – while in Block mode, the scroll bar disappears.

Line 25

Extra Information	This item determines what is displayed on the far right side of the status line (line 25) as follows: **None**: Nothing is displayed. **Response Time**: The time between when a user hits a function key and the next screen appears is displayed. **Cursor Location**: The current cursor location (row, column) is displayed.

Configure Recent Typing (6530)

Getting there

1 Open a 6530 terminal session.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click .
TouchUx	Tap the Gear icon and then select **Document Settings**.

2 Under **Productivity**, click **Configure Recent Typing**.

Recent typing is used to retain commonly entered lines for later re-use. When enabled, typing a character or pressing the up or down arrow keys opens an inline editor showing you commands you have previously typed – just the commands that start with the character you typed, or all commands if the up or down arrow is used on an empty prompt line. Since the inline editor is a normal edit box, you can then change the command as you require and press Enter to send it to the host.

You can bring up a full list of all typed in strings by clicking on the Recent Typing item in the Productivity section of the Session ribbon. You can then select one of the commands and send it to the host by double clicking on it.

NOTE: For information about creating and editing macros, using file transfer, logging, and other features, see the 6530 Help available on the Session ribbon Help group.

Record Recent Typing

Capture recent typing	Use this item to enable / disable recent typing entirely. If unchecked, all other elements are disabled.
Conversational mode capture	If checked, commands are recorded, and the **Inline Editing** item is enabled.
Inline editing	If checked, the inline editor appears when a character is typed or the up or down arrow is pressed while at a command prompt.
OSS mode capture	If checked, commands are recorded, and the **Inline Editing** item becomes enabled.
Inline editing	If checked, the inline editor appears when a character is typed or the up or down arrow is pressed while at a command prompt.
Block mode capture	If checked, fields that are typed into will also be stored as recent typing. Note the only way to enter a previously typed word/string into a field is through the **Recent Typing** box, which is opened by clicking on the **Recent Typing** item in the Productivity section of the Session ribbon.

Recent Typing Options

Maximum number of items in recent typing list	Use this item to set the number of commands to retain in the recent typing file.
Minimum size of item in recent typing list (characters)	Use this item to set the smallest command to retain in the recent typing file.
Clear recent typing list when disconnected	If checked, all saved recently typed items are discarded.
Load/save recent typing list on session startup/ exit	Use this item to indicate whether or not to save and load the recent typing list on startup and exit.

Performing a Trace

Your Technical Support analyst may ask you to trace Reflection events to troubleshoot problems. These instructions show how to perform traces on IBM 3270, IBM 5250, and VT sessions.

In this Section

Run a Trace for an IBM 3270 or 5250 Session

While troubleshooting a problem in an IBM 3270 or 5250 session, technical support may request that you obtain one or more traces. Three kinds of traces can be done: host-data, command, and HLLAPI.

Trace File Type	Description
Host-data trace (*.hst)	Captures information passed between a terminal, or printer, session and the host. This type of trace is useful when a host connection is working, but the terminal or printer session does not behave as expected. Host traces are not useful when a connection to the host cannot be established.
Command trace (*.cmd)	Captures actions within Reflection. Each action, such as clicking a button or entering text, represents an individual command. Command traces are useful in determining if commands are correct in a script, macro, or program using OLE automation. Command traces can also be used to determine which command to use when writing a script. Use a text editor to view the command trace and determine which commands are needed to accomplish the task.
HLLAPI trace	Enables you to see the HLLAPI calls the application is making, including return codes. (HLLAPI is an API specified by IBM for automating terminal tasks.)

To generate a host-data or command trace

1 Open a session or create a new session.

2 Open the Start Trace dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Reflection Ribbon	On the **Tools** ribbon, from the **Tracing** group, click **Start Trace**.
Reflection Browser	On the Reflection menu, choose **Tools**, **Trace**, and then **Start Trace**.
TouchUx	Tap the Wrench icon and then under **Trace**, select **Start Trace**.

3 In the Start Trace dialog box, specify a name for the trace file. If you have spoken with a support technician, use your service request number as the name of your trace file.

For this type of trace	Use this extension
Host data	.HST
Command	.CMD

4 Click **Save**.

"Tracing started..." displays in the Reflection status bar, indicating the trace is active.

5 Perform the actions that reproduce the problem you want recorded in the trace.

6 Stop the Trace.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
The Reflection Ribbon	On the **Tools** ribbon, from the **Tracing** group, click **Stop Trace**.
The Reflection Browser	On the Reflection menu, choose **Tools**, **Trace**, and then **Stop Trace**.
TouchUx	On the Reflection menu, tap the Wrench icon and then under **Trace**, select **Stop Trace**.

7 Upload the trace file as a binary file to http://upload.attachmate.com (http://upload.attachmate.com). If the problem relates to a service request you are currently working on with a technician, include the Micro Focus service request number with the trace and let the technician know when the file is uploaded.

To generate a HLLAPI trace

1 Click the Windows Start button.

2 In the Start Search box, type `win.ini` and press Enter to open your Win.ini file in Notepad.

3 Add the following two lines to the end of the Win.ini file:

```
[Reflection HLLAPI]
ExtTraceOn=1
```

4 In the Reflection Workspace, open a session or create a new session to connect to your IBM host.

5 Start the HLLAPI application.

6 Perform the actions that reproduce the problem you want recorded in the trace.

7 Close the HLLAPI application.

The trace file is automatically named HLL*.TMP, where * is a randomly generated hex number. The file is located in the PC's TEMP directory, if a TEMP directory has been defined in the System Environment settings. Otherwise, it is located in the root Windows directory.

8 Re-open the Win.ini file, and change the ExtTraceOn setting to zero by changing the last line of the ini file:

```
ExtTraceOn=0
```

9 Upload the trace file as a binary file to http://upload.attachmate.com (http://upload.attachmate.com). If the problem relates to a service request you are currently working on with a technician, include the Micro Focus service request number with the trace and let the technician know when the file is uploaded.

Perform an Event Trace (VT)

Your Technical Support analyst may ask you to perform an event trace. An event trace "captures" all communications activity (except for modem commands), and all keystrokes, commands, and menu and dialog box selections. This data is saved in an event file.

To use the trace data, you will need to process it to create a report of the data or to create a file that "plays" the trace.

To perform an event trace

1 Open the Start trace dialog box.

With a VT session open in the workspace, open the Start Trace dialog box as follows:

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Tools** tab, in the **Tracing** group, click **Start Trace**.
Reflection Browser	On the Browser Reflection menu, choose **Tools**, **Trace** and then **Start Trace**.
TouchUx	Tap the Wrench icon, and then under **Trace**, select **Start Trace**.

2 In the Start Trace dialog box, enter a path and file name for the event (`.rev`) file and click **Save**. (If you have spoken with a support technician, use your service request number as the name of your trace file.)

3 Perform the actions required to demonstrate the problem.

4 After the problem is demonstrated, click **Stop Trace** in the **Tracing** group (if using the Ribbon) or on the **Tools, Trace** menu (if using the Browser).

The trace data is saved in the event file.

5 Upload the trace file as a binary file to http://upload.attachmate.com (http://upload.attachmate.com). If the problem relates to a service request you are currently working on with a technician, include the Micro Focus service request number with the trace and let the technician know when the file is uploaded.

To process trace data

After creating the event file, follow these steps to create a report or a script that "plays" the trace.

1 Open the Process Event Trace dialog box.

With a VT session open in the workspace, open the Process Event Trace dialog box as follows:

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Tools** tab, in the **Tracing** group, click **Process Trace**.
Reflection Browser	In the search box, enter P and then, under **Actions**, select **Process Trace**.
TouchUx	Tap the Wrench icon and then, under **Trace**, select **Process Trace**.

2 Select how to process the trace:

To	Do this...
Create a Reflection Basic script that you can use to play the trace.	Select **Generate script.**
Create a report in a text-based file format.	Select **Generate report** and then select options to format the report under **Report format**. (See Process Event Trace Dialog Box (VT Sessions.) (page 422)

3 Click **OK**. The Open Events dialog box appears.

4 In the **File name** box, select the event file to process, and click **Open**.

- ◆ If you selected **Generate script**, the Save Event Commands dialog box opens.
- ◆ If you selected **Generate report**, the Save Event Report dialog box opens.

5 Enter the file name and click **Save**.

Scripts are saved as Reflection Basic .rbs files.

Reports are saved in .txt files. The report is automatically displayed after it is saved.

To play trace data

1 Open the Play Trace dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Reflection Ribbon	On the **Tools** ribbon, from the **Tracing** group, click **Play Trace**.
Reflection Browser	On the Reflection menu, choose **Tools**, **Trace**, and then **Play Trace**.
TouchUx	Tap the Wrench icon and then under **Trace**, select **Play Trace**.

2 In the Play Trace dialog box, select an event trace `.rbs` file and click **Open**.

Related Topics

- "Configure Connection Settings Dialog Box (VT)" on page 344
- "Configure Serial Device Port Dialog Box" on page 592

Process Event Trace Dialog Box (VT Sessions)

Getting there

With a VT session open in the workspace, open the Process Event Trace dialog box as follows:

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Tools** tab, in the **Tracing** group, click **Process Trace**.
Reflection Browser	In the search box, enter P and then, under **Actions**, select **Process Trace**.
TouchUx	Tap the Wrench icon and then, under **Trace**, select **Process Trace**.

This dialog box allows you to process a trace created when troubleshooting a problem in a VT session.

NOTE: For instructions that show how to trace events, process a trace, generate a trace report, or play a trace, see "Perform an Event Trace (VT)" on page 420

The options are:

Generate script	Create a report with a .rbs file extension in the folder you select. Use this option to process the trace (.rev) file into a Reflection Basic script file.
Generate report	Create a report with a .txt file extension in the folder you select. Use this option to process the trace (.rev) file into a text-based file format.

Report format

If you selected Generate report, you can also select any of these options:

Settings details and system information	Select to include settings and information about the operating system of your machine.
Timing	Select to put a time stamp beside each event item performed during the trace.
Display memory	Select to include all the information in the display memory buffer.
Network protocol details	Select to include details about the network protocol used for the connection.
Code page details	Select to include the code page information used by the PC.
Redact	Select to expunge sensitive information from traces. Specifically, this option replaces alpha characters with X's and numeric characters with 9's. Control and escapes sequences are not affected, only application data.
String syntax	Select the format used to display strings. Choose from Traditional, Visual Basic, or C string syntax.

6 Secure Connections

Reflection provides a variety of features to ensure the security of your communications when you are connecting over an unsecured network.

- ◆ "FIPS Mode" on page 425
- ◆ "Protecting Data and Information Privacy" on page 426
- ◆ "SSL/TLS Connections" on page 436
- ◆ "Secure Shell Connections" on page 436
- ◆ "Certificate Authentication (PKI)" on page 520
- ◆ "SOCKS or HTTP" on page 536
- ◆ "Security Properties Dialog Box" on page 542

FIPS Mode

When you run in FIPS mode, all connections are made using security protocols and algorithms that meet FIPS 140-2 standards. In this mode some standard connection options are not available.

To run Reflection in FIPS mode

1 Run the Group Policy editor using one of the following techniques:

- ◆ Type the following at the command line:

  Gpedit.msc

- ◆ In the **Active Directory Users and Computers** console, open the properties for an **Organizational Unit**, click the **Group Policy** tab, and edit or create a new policy object.

2 Install the Reflection template (ReflectionPolicy.adm) if you have not already done so.

> **NOTE:** For information about how to download and install the Reflection policy template, see Knowledge Base Article 7021501 (https://support.microfocus.com/kb/doc.php?id=7021501).

3 Under **Local Computer Policy** > **User Configuration** > **Administrative Templates**> **Reflection Settings**, disable the setting **Allow non-FIPS mode**.

What is FIPS 140-2?

The United States Government's Federal Information Processing Standard (FIPS) 140-2 specifies security requirements for cryptographic modules. Cryptographic products are validated against a specific set of requirements and tested in 11 categories by independent, U.S. Government-certified testing laboratories. This validation is then submitted to the National Institute of Standards and Technology (NIST), which reviews the validation and issues a certificate. In addition, cryptographic algorithms may also be validated and certified based on other FIPS specifications. The list of validated products and the vendor's stated security policy (the definition of what the module has been certified to do) can be found at: Cryptographic Module Validation Program.

IMPORTANT: If you are configuring Reflection to use FIPS mode, you should ensure that you are running a version that has met all FIPS 140-2 standards. Contact technical support for more information.

Related Topics

- "SSL/TLS Connections" on page 436
- "Secure Shell Connections" on page 436

Protecting Data and Information Privacy

Use the Trust Center to protect your working environment from information theft, and your data from potential damage caused by opening documents from non-trusted sources.

From the Trust Center, you can protect your data using the following methods.

- Set up trusted locations, from which you can safely open (and store) documents.
- Set up Information Privacy to mask sensitive data (such as credit card numbers) with privacy filters.
- Set up API and macro security to control access to the Reflection API and control the execution of actions invoked by a macro or API call.

Specify Trusted Locations Dialog Box

Getting there

1 Open **Workspace Settings**.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the the **File** menu or the Reflection button ⬡ (if using the Office 2007 Look and Feel), choose **Reflection Workspace Settings**.
Reflection Browser	On the Reflection menu, choose **Settings** and then **Reflection Workspace Settings**.
TouchUx	Tap the Gear icon and then select **Reflection Workspace Settings**.

2 Under **Trust Center**, click **Specify Trusted Locations**.

A trusted location is a directory that's designated as a secure source for opening files. By default, Reflection allows you to open documents only in directories specified as trusted locations in the Reflection settings.

During installation, Reflection specifies four default trusted locations on your local hard drive. The paths for three of these trusted locations cannot be modified or deleted. However, you can remove the trusted location for the user desktop (`...users\<user>\Desktop`). You can also add your own trusted locations to the list.

Trusted Locations

Open files only from trusted locations (recommended)	When selected, Reflection prompts you to save files to trusted locations.
Path	The complete path for the trusted location. You can change, edit, or delete any trusted locations you add.
Subfolders	Trust all folders located within the trusted location.
Description	When a path is selected, you can add text that will be associated with the trusted location.
Add New Location	Creates another box in the list for you to add the path for a new trusted location.
Allow trusted locations on my network (not recommended)	Select to add a network path to the list of trusted locations. It is recommended to leave this option unselected unless you are using VBA references to remotely located session documents, as shown in Set up VBA References.

Related Topics

◆ "Protecting Data and Information Privacy" on page 426

Set Up Information Privacy Dialog Box

Getting there

1 Open Workspace Settings.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **File** menu, or the Reflection button ⬙ (if using the Office 2007 Look and Feel), choose **Reflection Workspace Settings**.
Reflection Browser	On the Reflection menu, choose **Settings** and then **Reflection Workspace Settings**.
TouchUx	Tap the Gear icon and then select **Reflection Workspace Settings**.

2 Under **Trust Center**, click **Set Up Information Privacy**.

You can configure Information Privacy features to protect sensitive data so that it is not displayed on the screen or in productivity features, such as Screen History. You can choose from three methods for redacting Primary Account Number (PAN) data used for credit cards.

You can also redact other types of sensitive data and set other security features to protect your data.

Redacting Primary Account Numbers used for credit cards

You can redact credit card Primary Account Numbers (PANs) to meet "PCI DSS" on page 898 requirements (see PCI Security Standards Council). You can choose from three methods for redacting credit card PAN data: Simple Primary PAN Detection, Simple PAN Detection with Preceding Text, or Reflection PAN Detection.

Method	Use when	Considerations
Simple PAN Detection matches a credit card number sequence.	All of the credit card data in your host applications are displayed and entered in a "contiguous" fashion. You are only detecting PANs for the prepackaged major credit card issuers.	Easy to set up
Simple PAN Detection with Preceding Text matches preceding text (e.g., Account) followed by a credit card number sequence.	Same as above except credit card data in your host applications are always labeled in predictable ways.	Relatively easy to set up Avoids false positives
Reflection PAN Detection uses regular expressions to detect PANs.	You need to define custom card issuer patterns to detect, such as oil company or department store cards. PANs appear in a non-contiguous format or are entered using non-standard digit group separators. You want PAN detection to be especially "aggressive" or "greedy" in that any digit grouping on any screen should be considered for redaction, and you need to be able to redact without regard to what other text or digit separators may appear between single or groups of digits in the PAN.	Allows the greatest degree of flexibility and customization for unique detection needs Computationally-intensive— can degrade performance on PCs with limited processing power or memory The likelihood of "false positive" redaction is much greater with this method than the other two, especially if your host screens are very digit-laden

Redacting Other Types of Data and Requiring Secure Connections

You can redact other types of sensitive data like US Social Security Numbers and set other security features to require secure connections. You can also enable events that fire when PANs can be viewed by a user.

Do this...	If you need to...
Set up **Privacy Filters Redaction Rules** and **Privacy Filters**.	Redact certain patterns of data that are outside the realm of credit card formats (e.g., US Social Security numbers).
Set up **PCI DSS Rules**.	Require secure connections (as may be required for PCI DSS compliance).
	Fire API events that you can handle to create logs or perform other actions required for compliance.

NOTE

- You can use Privacy Filters together with Primary Account Number (PAN) detection. To improve performance, do not duplicate existing PAN patterns in privacy filters.
- Information Privacy settings do not apply to IBM host printer emulation.
- If redaction is enabled, HLLAPI functions are disabled to prevent access to unredacted data through HLLAPI.

For detailed explanations, instructions, and examples that show how to set up Information Privacy features, see the Reflection Desktop Deployment Guide.

Information Privacy Settings

Privacy Filters Redaction Rules

Use privacy filters when you need to:

- Redact certain patterns of data that are outside the realm of credit card formats (for example, US Social Security numbers or proprietary sensitive account numbers).
- Redact Primary Account Numbers (PANs) that are outside of a 13-16 digit range. (PAN detection does not detect PANs that are outside of this range.)

The redaction rules specify how to redact sensitive data, based on the filters that you specify in **Privacy Filters**.

Enable redaction (exported data only)	Redacts sensitive data so that it is not displayed in productivity features, such as Office Tools integration, Screen History, Recent Typing, and Auto Complete. This option also obscures data from the Print Screen and Cut/Copy/Paste commands.
Redact display data (Terminals Supported: IBM)	Redacts data on screens after you navigate out of the current field.
Redact data while typing (Terminals Supported: IBM)	Redacts sensitive data as you type it in.

Privacy Filters

Add	Opens the Add Privacy Filter dialog box where you can define the filter.
Modify	Opens the Modify Privacy Filter dialog box where you can modify the regular or simple expression that defines the filter.
Delete	Deletes the selected filter.

Primary Account Number (PAN) Redaction Rules

You can set up redaction rules to redact PANs (credit card numbers) that appear in screen histories, the clipboard, and Microsoft Office applications. You can also choose to redact PAN data displayed on screens, either as the PAN is typed or after it is entered.

Enable Redaction (exported data only)	Redacts sensitive data, based on the rules that you specify in **Primary Account Number (PAN) Detection Rules**.
Portion of PAN to redact	Specifies how many digits of the PAN to redact.
Redact display data (Terminals Supported: IBM)	Redacts data after it is entered.
Redact data while typing (Terminals Supported: IBM)	Redacts data as it is typed.
Do not store typed PANs	Prevents PAN data from being saved in an external file or any component that saves screen data. This includes the data saved for the Screen History, Recent Typing, Auto Complete, Auto Expand, and Macro Recording features. It also includes data returned by the Reflection API CreditCardRecognized event.

Primary Account Number (PAN) Detection Rules

Custom Detection Rules	Allow you to add, modify, or delete the regular expressions used by the PAN Detection methods to detect PAN data.
Reflection PAN detection	Allows you to set up regular expressions to detect PAN data.
	Reflection PAN Detection is the most flexible option for detecting PANs but is more difficult to configure that the other options. The likelihood of "false positive" redaction is much greater with this method than the other two, especially if your host screens are very digit-laden.
	Use this option when:

- You need to define custom card issuer patterns to detect, such as oil company or department store cards.
- PANs in your application appear in a non-contiguous format, such as multiple input fields of data arranged in a vertical table, or are entered using non-standard digit group separators.

NOTE: For more about how to use regular expressions to define rules or exceptions for PAN data, see the Reflection Desktop Deployment guide.

Custom Exception Expressions

Use regular expressions to define additional exclusion patterns that prevent false positives or preserve data that you do not want to redact.

NOTE: By default Reflection does not redact digit patterns such as North American phone numbers containing area code information and optional country code, common short date/time formats (MM/DD/YYYY, YYYY/MM/DD, HH:MM:SS, HH:MM, etc), and US Social Security numbers.

Simple PAN detection
Matches either a credit card number sequence (a 13-16 digit number) or preceding text (e.g., keywords like "Account") followed by a credit card number sequence.

This option is the easiest option to set up and works well for most applications.

Use Simple PAN detection when:

- All credit card data in host applications are always displayed and entered as a single continuous string (e.g. `1211-1441-1311-1551`).

- You need to redact account numbers only from: Visa, MasterCard, American Express, Discover, Diner's Club, Carte Blanche, Voyager, JCB, or enRoute. (If you need to detect other card issuers, use **Reflection PAN detection** or **Privacy Filters**.)

- All host application screens containing credit cards are very well defined, and credit card information is always "labeled" in predictable ways. (For instance, credit card numbers are always preceded by a label such as "Account: ").

Detect PANs based on 13-16 digit numbers with separators

Matches a credit card number sequence.

Detect PANs based on preceding text

If credit card data in your host applications are always labeled in predictable ways, using this option can help avoid false positives.

Matches preceding text followed by a credit card number sequence. To use this option, you will need to add the preceding text (e.g., `Account`) to the **Text Items** box.

Common Redaction Rules

You can configure Reflection to allow APIs to read redacted data or to allow copying of redacted data with a session.

Allow APIs to read redacted data
Allows programs or macros using the Reflection .NET and VBA APIs to read redacted data as clear text.

For example, you could set up Information Privacy features to mask credit card numbers so that users are unable to see them. With this option enabled, you can also run some automation that scrapes the screen and retrieves all the data on the screen, even the redacted data.

Allow copy of redacted data within sessions	Allows users to copy redacted data from a screen in an IBM session to another screen in the same session or to a screen in another IBM session.
	When enabled, users can select redacted data on the screen, and then copy and paste it to another location.
	For example, if a user is navigating a mainframe session in a workspace configured to redact credit card numbers and they receive a host screen that contains a credit card, it appears as a series of asterisks and numbers (e.g., ************3267). When this option is enabled, the user can copy this redacted credit card number, navigate a few more screens, and then paste the data.
	NOTE: When this option is selected, the **Wrap text to next input field** Clipboard setting is not supported and pasted text that exceeds the length of a field is truncated instead of being pasted to the next unprotected field.
Retain redacted data formatting	When **Allow copy of redacted data within sessions** is enabled, this option removes non-digit characters from a redacted string when it is pasted onto another screen.
	Select this option when you are copying redacted PAN data that spans more than one field from one IBM screen to another. If a Primary Account Number (PAN) spans several fields, and you copy redacted data from these fields, the information you copy may include additional characters that are not part of the PAN. When this option is selected, those characters are removed when the data is pasted.

PCI DSS Rules

You can configure Reflection to require secure connections for all network connections or for only wireless connections. You can also choose to fire a Reflection API event when an unredacted PAN (or credit card number) is displayed.

Do not require secure host connections	Allow non-secure connections, such as Telnet. Select this option only when testing or when your sessions do not require PCI DSS compliance.
Require secure host connections on all networks	Allows only secure connections, regardless of the type of network. This applies to wired, wireless, and VPN connections.
Require secure host connections on wireless networks	Allows non-secure connections on wired networks but requires secure connections for wireless networks.
	NOTE: VPN connections are not subject to the wireless restrictions. Because of VPN's inherent security, VPN connections are handled in the same way as wired connections. To secure VPN connections, choose the **Require secure host connections on all networks** option.

Enable API events when PANs are viewed by the user	Fires the *CreditCardRecognized* .NET API and VBA event when unredacted PAN data is copied from the terminal to the clipboard or to a productivity tool. For IBM systems, the event is also fired when unredacted PAN data is displayed on the screen.
	You can handle this event to create logs or perform other actions required for compliance. (See the Reflection VBA Guide or the Reflection .NET API Guide.)
	NOTE: This event is fired only when a PAN is copied or displayed in its entirety ("in the clear"). It is not fired when only redacted PANs are copied or displayed.

Add (or Modify) Privacy Filter Dialog Box

Getting there

1 Open Workspace Settings.

The steps depend on your .

User Interface Mode	Steps
Ribbon	On the **File** menu or the Reflection button (if using the Office 2007 Look and Feel), choose **Reflection Workspace Settings**.
Reflection Browser	On the Reflection menu, choose **Settings** and then **Reflection Workspace Settings**.
TouchUx	Tap the Gear icon and then select **Reflection Workspace Settings**.

2 Under **Trust Center**, click **Set Up Information Privacy**.

3 Under **Privacy Filters**, click **Add** or **Modify**.

Description	Enter the name of the filter. This is displayed under **Privacy Filters** in the Set Up Information Privacy dialog box.
Regular expression	Enter (or modify) the regular expression that defines the filter.
	NOTE: For more about how to use regular expressions to define rules or exceptions for PAN data, see the Reflection Desktop Deployment Guide.
Simple expression	Enter (or modify) the simple expression that defines the filter. For example, the following filter redacts US Social Security numbers:
	###-##-####

Add (or Modify) Custom Detection Rule or Exception Dialog Box

Getting there

1 Open Workspace Settings.

The steps depend on your .

User Interface Mode	Steps
Ribbon	On the **File** menu or the Reflection button (if using the Office 2007 Look and Feel), choose **Reflection Workspace Settings**.
Reflection Browser	On the Reflection menu, choose **Settings** and then **Reflection Workspace Settings**.
TouchUx	Tap the Gear icon and then select **Reflection Workspace Settings**.

2 Under **Trust Center**, click **Set Up Information Privacy**.

3 Under **Reflection PAN detection**, next to either **Custom Detection Rules** or **Custom Exception Expressions**, click **Add** or **Modify**.

Description	Enter the name of the rule or exception. This is displayed under **Reflection PAN detection** in the Set up Information Privacy dialog box.
Regular expression	Enter (or modify) the regular expression that defines the custom rule or exception.
	NOTE: For more about how to use regular expressions to define rules or exceptions for PAN data, see the Reflection Desktop Deployment Guide.

Set Up API and Macro Security Dialog Box

Getting there

1 Open Workspace Settings.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **File** menu or the Reflection button (if using the Office 2007 Look and Feel), choose **Reflection Workspace Settings**.
Reflection Browser	On the Reflection menu, choose **Settings** and then **Reflection Workspace Settings**.
TouchUx	Tap the Gear icon and then select **Reflection Workspace Settings**.

2 Under **Trust Center**, click **Set Up API and Macro Security**.

From this dialog box, you can enable the Reflection .NET API, and specify corresponding settings.

NOTE: If you need to use the API in multiple instances of Reflection simultaneously, use layouts. You can specify different settings for the **IPC channel name** for each layout in the **Layout Settings** dialog box.

API Settings*

Disable API	Select to prevent custom applications from accessing this installation of Reflection.
Legacy API preference	Use this setting to determine if Reflection legacy macros are supported, and to determine which legacy API has preference for the GetObject() method used to retrieve API COM objects. Reflection supports multiple APIs, but can accept GetObject() calls for only one type of legacy API object at a time.

Select	If you
No Legacy API	Don't use legacy Reflection macros, or if your code doesn't use GetObject() to access legacy API COM objects.
Reflection	Use legacy Reflection macros, or if you use GetObject() to access legacy Reflection API COM objects. Each session document that you subsequently open or create has legacy macro capability; it includes a legacy VBA project in addition to the standard VBA project in the Visual Basic Editor. **NOTE:** Legacy API support is provided in all Reflection settings files that you open in the workspace (including settings files saved as Reflection session documents), regardless of this setting.
Extra!	Use GetObject() to access Extra! API COM objects.

Action Permissions

Specify what you want to happen if an action that has been restricted through Group Policy or the Permissions Manager is initiated through a macro or API call.

Require elevated rights	Select to control restricted actions with User Account Control (UAC).
Execute the action	Select to run restricted actions that are initiated through a macro or API call as expected. The same actions won't run if they are initiated through the user interface.

Related Topics

- "Layout Settings Dialog Box" on page 141
- "Using Layouts" on page 141
- "Protecting Data and Information Privacy" on page 426

SSL/TLS Connections

In this Section

SSL/TLS Overview

The Secure Sockets Layer protocol (SSL) and its compatible successor, the Transport Layer Security protocol (TLS), enable a client and server to establish a secure, encrypted connection over a public network. When you connect using SSL/TLS, the client authenticates the server before making a connection, and all data passed between the client and the server is encrypted. Depending on the server configuration, the server may also authenticate the client.

Authentication is accomplished by sending an X.509 security certificate. Authentication occurs automatically and invisibly as the first step of establishing an SSL/TLS connection. SSL/TLS connections require the client to authenticate the server. It is optional for the server to authenticate the client.

Once an encrypted connection is established, data is transmitted using the encryption level you have specified.

Supported Cryptographic Algorithms

Supported versions are: TLS version 1.3 (IBM, VT, and FTP connections only), TLS version 1.2, TLS version 1.0 (the default) and SSL version 3.0. The list of cipher suites available for a given connection depends on the SSL/TLS version you specify, the encryption strength setting, and whether or not you are configured to run in FIPS mode.

For TLS connections, Elliptic Curve Cryptography (ECC) is supported in IBM, VT, and FTP sessions. Currently, only prime curves are supported for Elliptic Curve Cryptography.

Secure Shell Connections

In this Section

Secure Shell Overview

You can configure Secure Shell connections when you need secure, encrypted communications between a trusted host and your PC over an insecure network. Secure Shell connections ensure that both the client user and the host computer are authenticated; and that all data is encrypted. Passwords are never sent over the network in a clear text format as they are when you use Telnet, FTP, or rlogin.

The following cryptographic algorithms are supported:

Data Encryption Standards

Encryption protects the confidentiality of data in transit. This protection is accomplished by encrypting the data before it is sent using a secret key and cipher. The received data must be decrypted using the same key and cipher. The cipher used for a given session is the cipher highest in the client's order of preference that is also supported by the server. You can use the **Encryption** tab of the **Reflection Secure Shell Settings** dialog box to specify which ciphers the Secure Shell connection should use.

The following data encryption standards are supported:

 ◆ Arcfour, Arcfour128, and Arcfour258 (stream mode)

 ◆ TripleDES (168-bit) CBC mode

 ◆ Cast (128-bit)

 ◆ Blowfish (128-bit) CBC mode

 ◆ AES (also known as Rijndael) (128-, 192-,or 256-bit) CBC mode and CTR mode

Data Integrity

Data integrity ensures that data is not altered in transit. Secure Shell connections use MACs (message authentication codes) to ensure data integrity. The client and server independently compute a hash for each packet of transferred data. If the message has changed in transit, the hash values are different and the packet is rejected. The MAC used for a given session is the MAC highest in the client's order of preference that is also supported by the server. Reflection supports the following MAC standards:

 ◆ hmac-sha1

 ◆ hmac-md5

 ◆ hmac-sha1-96

 ◆ hmac-md5-96

 ◆ hmac-ripemd-160

 ◆ hmac-sha256

 ◆ hmac-sha2-256

 ◆ hmac-sha512

 ◆ hmac-sha2-512

Digital Signatures

Digital signatures are used for public key authentication (including certificate authentication). The authenticating party uses the digital signature to confirm that the party being authenticated holds the correct private key. The Secure Shell client uses a digital signature to authenticate the host. The Secure Shell server uses a digital signature to authenticate the client when public key authentication is configured. Reflection supports the following digital signature algorithms:

- x509v3-rsa2048-sha256
- x509v3-sign-rsa
- x509v3-sign-dss
- ssh-rsa-sha2-256@attachmate.com
- ssh-rsa
- ssh-ds

Understanding Secure Shell

This diagram outlines the basic steps involved in creating a Secure Shell channel and using it to transmit data securely.
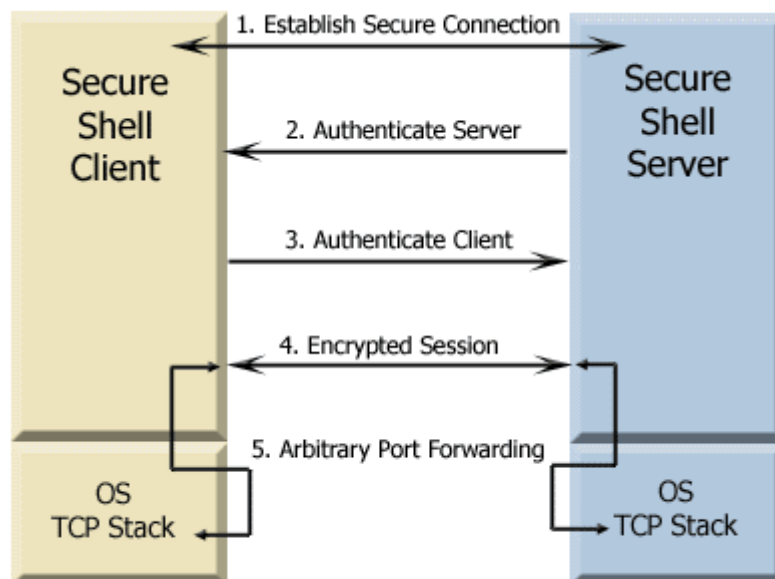
1 **Establish a secure connection.**

The client and server negotiate to establish a shared key and cipher to use for session encryption, and a hash to use for data integrity checking.

2 **Authenticate the server.**

Server authentication enables the client to confirm the identity of the server. The server has only one chance to authenticate to the client during the authentication process. If this authentication fails, the connection fails.

3 **Authenticate the client.**

Client authentication enables the server to confirm the identity of the client user. By default, the client is allowed multiple authentication attempts. The server and client negotiate to agree on one or more authentication methods.

4 Send data through the encrypted session.

Once the encrypted session is established, all data exchanged between the Secure Shell server and client is encrypted. Users now have secure remote access to the server and can execute commands and transfer files securely through the secure channel.

5 Use port forwarding to secure communications between other clients and servers.

Port forwarding, also known as tunneling, provides a way to redirect communications through the Secure Shell channel of an active session. When port forwarding is configured, all data sent to a specified port is redirected through the secure channel.

Connect using Secure Shell (SSH)

You can configure Secure Shell connections when you need secure, encrypted communications between a trusted host and your PC over an insecure network. Secure Shell connections ensure that both the client user and the host computer are authenticated; and that all data is encrypted. Passwords are never sent over the network in a clear text format as they are when you use Telnet, FTP, or rlogin. You can use this procedure to connect securely to UNIX and Linux hosts.

NOTE: Secure Shell connections are available for VT terminal sessions.

Before you start

By default, Secure Shell connections use public key authentication for the host and username/ password authentication for the user. To configure a connection using these defaults, you need to make sure your system has a Secure Shell server or servers and that you know the following information:

- The host name.
- The User name and password.
- The port used by the Secure Shell server (the default is 22).

To configure a secure terminal session using Secure Shell (SSH)

1 Open the **Create New Document** dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	From the Quick Access Toolbar, click the **New Document** 📄 button.
TouchUx	Tap the Folder icon and then under **File**, select 📄 **New**.

2 From the **Create New Document** dialog box, select the **VT Terminal** template and click **Create**.

3 In the **Create New** dialog box, under **Connection**:

- Select **Secure Shell**.

The Port value changes to 22, which is the standard port for Secure Shell connections. If you need to connect to a different port, select **Configure additional settings**, or use the procedure below to change the default Secure Shell settings.

- ◆ (Optional) Enter the **Host name/IP address.** If you omit this, you will be prompted for a host name when you connect.
- ◆ (Optional) Enter your **User name**. If you omit this, you will be prompted for a user name when you connect.

4 Click **OK**.

5 The first time you connect, you are prompted to verify the host hey authenticity. Verify the host key fingerprint and select **Always**.

NOTE: Host authentication (performed with public key authentication) enables the Secure Shell client to reliably confirm the identity of the Secure Shell server. If the host public key is not installed on the client, the host fingerprint is displayed and users are prompted to contact the system administrator to verify the fingerprint. This confirmation prevents risk of a "man-in-the-middle" attack, in which another server poses as the host. After the host key is added to the client, Micro Focus Reflection Desktop can authenticate the server without requiring user confirmation, and the unknown host prompt does not appear again. The key is saved in a file called `known_hosts`, which is created in the folder `%userprofile%\Documents\Micro Focus\Reflection\.ssh`.

---

6 When prompted, enter your password.

7 Click the **Save** button on the **Quick Access** toolbar and save the session document.

The file is saved in `[PersonalFolder]\Micro Focus\Reflection\`.

To configure username and password prompts to appear in the terminal window

1 Open a session that you have configured to use Secure Shell. Disconnect if you are connected.

2 Open the **Document Settings** dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click .
TouchUx	Tap the Gear icon and then select **Document Settings**.

3 Under **Host Connection**, click **Configure Connection Settings**.

4 Under **Connection Options**, select **Handle SSH user authentication in terminal window**.

To configure non-default Secure Shell settings

1 Open a session that you have configured to use Secure Shell. Disconnect if you are connected.

2 Open the **Document Settings** dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ⬚.
TouchUx	Tap the Gear icon and then select ⬚ **Document Settings**.

3 Under **Host Connection**, click **Set up Connection Security**.

4 In the **Reflection Secure Shell Settings** dialog box, configure any non-default settings and then click **OK**.

NOTE

- When you click OK, changes to the default settings are saved in the Secure Shell `config` file in `[PersonalFolder]\Micro Focus\Reflection\.ssh`

- If you want to deploy the session to all users of a computer, first rename the `config` file to `ssh_config` and the `known_hosts` file to `ssh_known_hosts`.

Related Topics

- "Configure Secure Shell Settings" on page 441
- "Connect Using Secure Shell (FTP Client)" on page 783
- "Managing Host Keys" on page 449

Configure Secure Shell Settings

In most cases Reflection will connect to your host and allow you to log in with your password using the default Secure Shell configuration. Use the **Reflection Secure Shell Settings** dialog box if you need to configure alternate user authentication methods or to make other changes to your Secure Shell configuration.

To modify the Secure Shell settings for a terminal session

1 Open the terminal session you want to modify.

2 Disconnect from the host.

3 Open the Document Settings dialog box.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ⬚.
TouchUx	Tap the Gear icon and then select ⬚ **Document Settings**.

4 Click **Configure Connection Settings**.

5 Under **Network Connection Type**, select **Secure Shell**.

6 Under **Connection Options**, enter a host name.

7 (Optional) Specify a value for **SSH configuration scheme**.

If you leave this blank, changes you make to your Secure Shell settings are saved to Secure Shell configuration file under the current host name, and the settings you configure are applied by default to all Secure Shell connections to this host. If you specify a scheme name, changes you make to your Secure Shell settings are saved to the Secure Shell configuration file under the specified scheme name, and the settings you configure are applied to subsequent connections whenever you specify this scheme name.

8 Click **Security**.

9 Use the **Reflection Secure Shell Settings** dialog box to configure your settings, then click **OK**.

NOTE: Changes you make to the default values are saved to the Secure Shell configuration file when you click **OK**.

Related Topics

Authentication

Authentication is the process of reliably determining the identity of a communicating party. Identity can be proven by something you know (such as a password), something you have (such as a private key or token), or something intrinsic about you (such as a fingerprint). Secure Shell connections require both host (server) and user (client) authentication. By default the host authenticates to the user using its private key, and then the user authenticates to the host using a password.

In this Section

Server Authentication using Public Keys

Secure Shell session support two types of server authentication: public key and certificate (a special form of public key authentication).

When public key authentication is used for host authentication, the following sequence of events takes place.

1. The Secure Shell client initiates a connection.

2. The server sends its public key to the client.

3. The client looks for this key in its trusted host key store.

If the client	This occurs
Finds the host key, and the client copy matches the key sent by the server	Authentication proceeds to the next step.
Does *not* find the host key	The client displays a message that the host is unknown and provides a fingerprint of the host key. If the client is configured to allow the user to accept unknown keys (the default), the user can accept the key, and authentication proceeds to the next step.
	If strict host key checking is enforced, the client ends the connection.
Finds a host key, and the client copy *doesn't* match the key sent by the server	The client displays a warning that the key doesn't match the existing key and displays the fingerprint of the key sent by the server. If the client is configured to allow the user to accept unknown keys (the default), the user can accept the new key.
	If strict host key checking is enforced, the client ends the connection.

4. To confirm that the server actually holds the private key that corresponds to the received public key, the client sends a challenge (an arbitrary message) to the server and computes a hash based on this message text.

5. The server creates a digital signature based on the challenge message. To do this, the server independently computes the message hash, and then encrypts the computed hash using its private key. The server attaches this digital signature to the original challenge and returns this signed message to the client.

6. The client decrypts the signature using the public key and compares the hash with its own computed hash. If the values match, host authentication is successful.

Connection Reuse in Secure Shell Sessions

Connection reuse enables additional Secure Shell sessions to be added to an already established Secure Shell connection. A simple analogy for this is a fiber optic cable, in which the outside pipe represents the connection, through which the various fiber-optic strands (the sessions and tunnels) are routed. The additional sessions can be new terminal sessions, new SFTP file transfer sessions, forwarded X11connections, any communications configured for port forwarding through the SSH tunnel, or any connection established using one of the Secure Shell command line utilities.

When you reuse an established Secure Shell connection, you don't need to repeat the authentication process. The new session always uses all the Secure Shell settings configured for the initial connection. Any differences in authentication methods, cipher or MAC settings, or port forward definitions are ignored.

Connection reuse is enabled by default for all Secure Shell connections from the user interface. You can disable this feature by clearing the **Reuse existing connection if available** check box on the **General (page 469)** tab of the Secure Shell Settings dialog box.

After you have established a connection in which **Reuse existing connection if available** is enabled, subsequent Secure Shell sessions reuse the established connection if all of the following conditions are true:

- The host name in the new session must exactly match the host name in the established connection.
- The user name in the new session must exactly match the user name in the established connection.
- The port number in the new session must be the same as the port number in the established connection. (This condition will be true by default.)
- If the original session is configured to use an SSH configuration scheme (page 485) that is different from the host name, the new session must be configured to use the same scheme.

NOTE: If you are using command line utilities to make SSH connections, additional conditions must be met in order to reuse existing connections. These are outlined below.

Connection Reuse in Command Line Sessions

Connection reuse is useful for command line operations in which Secure Shell connections are required, numerous small operations are needed between a client and a single server, and the authentication and key exchange time interval is a significant part of the total connection time. This would be the case if you need to transfer multiple small files, or execute simple operating system commands that do not result in large quantities of returned output. In these cases it might be advantageous to create the original SSH connection using the **ssh** (or **ssh2**) command line utility, and then reuse the connection with subsequent command line utility operations.

By default, connection reuse is disabled for the Secure Shell client command line utilities: **ssh** (page 505) , **scp** (page 515) , **sftp** (page 509) , **scp2**, and **sftp2**. To enable connection reuse with any of these command line utilities, you must use one of the following techniques.

- Add the switch " `-o ConnectionReuse=yes`" to each command line. You must use this switch when you establish the initial connection, and in all subsequent command lines that you want to reuse the initial connection. For example, with the following commands, the **sftp** connection will reuse the connection established by the **ssh** command.

  ```
  ssh "-o connectionReuse=yes" myuser@myhost
  sftp "-o connectionReuse=yes" myuser@myhost
  ```

- In the DOS command window (or at the beginning of a batch script file), set the environment variable SSHConnectionReUse as shown here:

  ```
  set SSHConnectionReUse=yes
  ```

If conflicting settings are present, the -o switch takes precedence.

NOTE

- OpenSSH servers support a MaxStartups parameter that can be used to limit the number of concurrent unauthenticated sessions. This setting will affect the number of sessions you can establish that reuse an existing connection. When you have reached the maximum number of

sessions specified in the MaxStartups parameter, all subsequent sessions will require a separate SSH connection with authentication. Contact your ssh server administrator, if you need to establish more concurrent unauthenticated sessions than are currently allowed.

◆ Command line utilities cannot be configured for connection reuse in the Secure Shell configuration file (page 484). The **ConnectionReuse** keyword in this file is always ignored by the Secure Shell command line utilities, even when the **-H** switch is used to specify an SSH configuration scheme (page 485) that includes this setting

Client Authentication Methods

The Secure Shell Client supports the Public Key, Keyboard Interactive, and Password methods of user authentication. Use the Secure Shell Settings (page 469) dialog box to configure your authentication preferences. You must select at least one authentication method. When more than one method is selected, the Secure Shell Client tries to authenticate in the order you specify. By default, Reflection attempts Public Key authentication first, followed by Keyboard Interactive, and then Password.

NOTE: The Public Key and GSSAPI authentication methods require both server and client configuration.

Authentication method	Description
Password	Prompts the client user for the login password for that user on the Secure Shell server host.
	The password is sent to the host through the encrypted channel.
Keyboard interactive	Supports any procedure in which authentication data is entered using the keyboard, including simple password authentication, thereby enabling the Secure Shell client to support a range of authentication mechanisms, such as RSA SecurID tokens or RADIUS servers.
	A client administrator could, for example, configure keyboard interactive authentication to handle situations in which multiple prompts are required, such as for password updates.
	Keyboard data is sent to the host through the encrypted channel.
Public Key	Relies upon public/private key pairs. To configure public key authentication, each client user needs to create a key pair and upload the public key to the server. If the key is protected by a passphrase, the client user is prompted to enter that passphrase to complete the connection using public key authentication.

Related Topics

◆ "General (Secure Shell Settings)" on page 469

Public Key Authentication

Public key authentication relies on public/private key pairs. Public key authentication can be used for both server (host) and client (user) authentication. To configure public key authentication for the Secure Shell client, you create (or import) a key pair for your client computer, then upload the public

key to your host(s). You can create and manage public keys for client authentication using either the **User Keys (page 472)** tab in the Reflection Secure Shell Settings dialog box, or the Reflection Key Agent (page 452). Depending on how you have configured your key, you may be prompted to enter a passphrase in order to complete a connection using public key authentication.

One form of public key authentication is accomplished using X.509 certificates. Reflection can be configured to authenticate using certificates managed by the "Reflection Certificate Manager" on page 528 and/or the Windows Certificate Manager. Public Key authentication must be enabled if you use certificates for authentication.

How Public Key Authentication Works

Public key cryptography uses a mathematical algorithm with a public/private key pair to encrypt and decrypt data. One of the keys is a public key, which can be freely distributed to communicating parties, and the other is a private key, which should be kept secure by the owner of the key. Data encrypted with the private key can be decrypted only with the public key; and data encrypted with the public key can be decrypted only with the private key.

When keys are used for authentication, the party being authenticated creates a digital signature using the private key of a public/private key pair. The recipient must use the corresponding public key to verify the authenticity of the digital signature. This means that the recipient must have a copy of the other party's public key and trust in the authenticity of that key.

In this Section

- "Managing User Keys" on page 446
- "Managing Host Keys" on page 449
- "Reflection Key Agent" on page 452

Managing User Keys

In this Section

- "Configure Public Key Authentication" on page 446
- "Add Keys to Your User Keys List" on page 447
- "Upload Client Public Keys to the Server" on page 448
- "Change a User Key Passphrase" on page 448
- "Export a User Key" on page 449

Configure Public Key Authentication

The following procedures configure client authentication using public keys.

To configure the client for public key authentication

1 Open the **Reflection Secure Shell Settings dialog box (page 483)**.

2 From the **General** tab, make sure that **Public Key** is selected under **User Authentication**. (If you want to ensure that only public key authentication is used, clear the other options.)

3 Click the **User Keys** tab. In the **Use** column, select the key or keys you want to use to authenticate to the currently specified host.

NOTE: To add keys to this list, see Add Keys to your User Key list (page 447).

4 Click **OK**.

To configure the server for public key authentication

◆ Upload the public key(s) to the host(s) (page 448).

Add Keys to Your User Keys List

The **User Keys (page 472)** tab of the Reflection Secure Shell Settings dialog box displays a list of keys you can use for public key (page 446) authentication. You can add keys to the list by creating new keys or importing existing keys.

To create a new key pair using Reflection

1 Open the **Reflection Secure Shell Settings dialog box (page 483)**.

2 Click the **User Keys** tab.

3 Click **Generate Key**.

4 Specify a key type and key length.

5 Either specify a "passphrase" on page 898, or select **No passphrase**.

CAUTION: If you select **No passphrase**, the private key saved to your computer is unencrypted, and anyone who gains access to this key will be able to use it to authenticate as you.

6 Click **Create**.

By default, keys are created in your user .ssh folder (page 900). The default private key name identifies the key type, size, and the client host name. The public key is saved to the same location using the private key name with an added *.pub file extension.

To create a new key pair using the Key Agent

1 Start and unlock the Reflection Key Agent. (From the Windows Start menu, go to **Programs** > **Micro Focus>Reflection> Utilities** > **Key Agent**.)

2 Click **Generate Keys**.

3 Specify a key name, key type, and key length, and click **OK**.

NOTE: Keys you create using the Key Agent are stored by the agent in encrypted form.

To Import keys into the Reflection key store

1 Open the **Reflection Secure Shell Settings dialog box (page 483)**.

2 Click the **User Keys** tab.

3 Click **Import**.

4 Browse to locate the private key you want to import. Each key pair includes two files, one with a *.pub extension and one with no file extension. The private key is the file with no extension.

NOTE: Imported keys are copied to the Reflection key store located in your user .ssh folder (page 900).

Upload Client Public Keys to the Server

Use the **Upload** button on the **User Keys** tab to upload a public key to the Secure Shell server. The public key is transferred using the secure SFTP protocol. You will need the ability to use password authentication (or another authentication method) in order to upload the public key. Once the public key is successfully uploaded, you may disable other authentication methods.

To upload a key

1 Open the **Reflection Secure Shell Settings** dialog box (page 483).

2 Select a key from the **User Keys** tab and click **Upload**. (The **Upload** button is not available if no key is selected, or if you have selected a certificate.)

3 If prompted, enter the host name, the name of the user who will authenticate, and the user password.

4 After the secure connection to the host has been established, a dialog box appears, displaying information about where on the host Reflection will upload this key. In most cases you do not need to change these settings. See the notes below for more information.

The **Upload Public Key** dialog box displays information about the transfer.

5 Click **OK** to close this dialog box.

NOTE

◆ Keys uploaded to hosts running Reflection for Secure IT, F-Secure, and SSH Communications (SSH Tectia) servers are exported using RFC 4716 compliant format. By default these are installed to the user's `.ssh2` directory and an appropriate **Key** entry is made in the `authorization` file. If this file did not previously exist, it is created and given appropriate file permissions.

◆ Keys uploaded to hosts running OpenSSH servers are exported using OPENSSH format. By default they are added to the `authorized_keys` file located in the user's `.ssh` directory. If this file did not previously exist, it is created and given appropriate file permissions.

Change a User Key Passphrase

You can change the "passphrase" on page 898 used to protect a user key.

To change the passphrase.

1 Open the **Reflection Secure Shell Settings** dialog box (page 483).

2 Click the **User Keys** tab and select a key from the list.

3 Click **Change Passphrase**. (This button is not available if no key is selected, or if you have selected a certificate managed by either the Reflection Certificate Manager or the Windows Certificate Manager.)

Export a User Key

Use the procedure below to export your user keys to a new location and/or format.

NOTE: If you want to upload a public key to a Secure Shell server, you do not need to use this procedure. Use the **Upload** button to do this in a single step. Reflection automatically determines the correct key format for the server you specify. See Uploading Keys to the Server (page 448) for more information.

To export a key

1 Open the **Reflection Secure Shell Settings** dialog box (page 483).

2 From the **User Keys** tab, select a key and click **Export**. (This button is not available if no key is selected, or if you have selected a certificate managed by either the Reflection Certificate Manager or the Windows Certificate Manager.)

3 Enter the "passphrase" on page 898 for the selected key.

4 (Optional)

To	Do this
Include the private key in the export	Select **Export Private Key**.
Export the key in OpenSSH format	Select **Save in OpenSSH format**.

5 From the **Public Key Filename** dialog box, specify a name and location for the exported key.

6 Click **Save**.

Managing Host Keys

In this Section

Configure Host Key Checking

Use this procedure to specify how Reflection should behave when connecting to an unknown host.

To configure host key checking

1 Open the **Reflection Secure Shell Settings** dialog box (page 483).

2 Click the **Host Keys** tab.

3 Click **Enforce strict host key checking**.

4 Select one of the following options:

Select	To
Ask User (default)	Display the Host Key Authenticity (page 451) confirmation dialog box when you connect to an unknown host.
Yes	Enforce strict host key checking — Reflection does not connect if the host is not a "trusted host" on page 900. Before you can connect, you must add the host key to your list of trusted host keys.
No	Prevent enforcement of strict host key checking — Reflection connects without displaying a confirmation dialog box. The host key is not added to the list of trusted keys.

NOTE

◆ **Enforce strict host key checking** has no effect when the host has been configured to authenticate using X.509 certificates. If a host presents a certificate for host authentication and you do not have the required CA certificate in your Trusted Root store, the connection fails.

◆ Changes you make to this setting are saved to the currently specified SSH configuration scheme (page 485).

◆ Secure Shell settings are saved to the Secure Shell configuration file (page 484). You can also configure Secure Shell settings by editing this file manually in any text editor. The keyword (page 486) used to configure this setting is **StrictHostKeyChecking**.

Related Topics

◆ "Host Key Authenticity Dialog Box" on page 451

◆ "The Known Hosts File" on page 451

Configure the Preferred Host Key Type

Use **Prefer ssh keys over certificates** to specify the order of preference for host key algorithms. This setting is useful when the server is configured for both certificate and standard host key authentication. SSH protocol allows only one attempt to authenticate the host. If the host presents a certificate, and the client is not configured for host authentication using certificates, the connection fails. (This is different from user authentication, in which multiple authentication attempts are supported.)

To configure the preferred host key type (standard SSH keys or certificates)

1 Open the Reflection Secure Shell Settings dialog box (page 483).

2 Click the **Host Keys** tab.

3 To have the host use standard host keys for authentication, select **Prefer ssh keys over certificates**.

-or-

To use certificates for authentication, clear **Prefer ssh keys over certificates**.

- Changes you make to this setting are saved to the currently specified SSH configuration scheme (page 485).

- Secure Shell settings are saved to the Secure Shell configuration file (page 484). You can also configure Secure Shell settings by editing this file manually in any text editor. The keyword used to configure this setting is **HostKeyAlgorithms**.

The Known Hosts File

The Reflection Secure Shell Client maintains a list of known hosts in the known hosts file. Reflection supports both user-specific and global known hosts files.

The user known hosts file	The user-specific known hosts file is called `known_hosts` and is located in the user's .ssh folder (page 900). This is the default known hosts file. Reflection automatically updates this file when: • You update the **Trusted Host Keys** list in the **Host Keys (page 477)** tab of the Secure Shell settings dialog box. - or - • You connect to a previously unknown host and answer **Always** in response to the **Host Key Authenticity (page 451)** prompt.
The global known hosts file	System administrators can add a system-wide known hosts file named `ssh_known_hosts` to the "Reflection global ssh folder" on page 899. In this location the known hosts file provides a list of hosts for all users of the PC. Keys in this list can be viewed, but not edited in the **Global Host Keys** list in the **Host Keys (page 477)** tab of the Secure Shell settings dialog box.

Related Topics

- "Configure Host Key Checking" on page 449

- "Deploy Secure Shell Settings with a Companion Installer" on page 503

Host Key Authenticity Dialog Box

This confirmation dialog box appears if the host you are connecting to is not a "trusted host" on page 900. Do you want to trust this new host key and continue connecting?

Host authentication enables the Secure Shell client to reliably confirm the identity of the Secure Shell server. This authentication is done using public key authentication. If the host public key has not previously been installed on the client, the first time you attempt to connect you see a message indicating that this is an unknown host. This message includes a fingerprint that identifies the host. To be sure that this is actually your host, you should contact the host system administrator who can confirm that this is the correct fingerprint. Until you know that the host is actually your host, you are at risk of a "man-in-the-middle" attack, in which another server poses as your host.

The options are:

Always	Make the connection and add this host to the list of trusted hosts. You will not see this prompt for subsequent connections to the same host unless you remove the host from the trusted host list, or the host key changes.
Once	Make the connection but do not add the host to the trusted host list. You will see this prompt again the next time you make a connection to the same host.
No	Do not make the connection and do not add the host to the trusted host list.

Reflection Key Agent

The Reflection Key Agent is a tool for creating and managing Secure Shell user keys. The Key Agent:

- Stores keys securely in encrypted form.
- Enables you to access all stored keys and certificates with a single passphrase. Because keys are decrypted and stored in memory, only your initial passphrase is required. The agent handles all subsequent authentication using your stored keys and certificates.
- Supports agent forwarding to additional Secure Shell servers. This enables public key authentication to be used for additional Secure Shell connections without transporting the private key.
- Provides tools for key and certificate management including: creating new keys, importing existing keys, importing certificates from the Windows and Reflection certificate stores, deleting keys, and uploading the public key file to a specified server in the appropriate format.
- Maintains a log file to aid in troubleshooting.

In this Section

Start the Key Agent

You can start the Reflection Key Agent from the Windows **Start** menu or from any Reflection or InfoConnect application that supports Secure Shell connections.

NOTE: Whenever the Key Agent is running, the **Key Agent** icon is visible in the Windows system tray.

To start the agent the first time

1 In the Windows **Start** menu, select the **Key Agent**.
2 Enter a passphrase (page 459). Use this phrase whenever you want to unlock the agent.

To start the agent from the Windows Start menu

1 In the Windows **Start** menu, select the **Key Agent**.

2 Click **Unlock** to unlock the agent.

To start the agent from your Reflection Application

1 Open the **Reflection Secure Shell Settings** dialog box.

2 Go to the **User Keys** section, and click **Launch Key Agent**.

3 Click **Unlock** to unlock the agent.

-or-

◆ Start a connection that is configured to use a key stored in the Key Agent.

If the agent is not already running, Reflection launches it automatically and displays a prompt to unlock the agent.

Related Topics

◆ "Key Agent Passphrase" on page 459

◆ "Lock or Unlock the Key Agent" on page 459

◆ "Hide and View the Key Agent" on page 460

◆ "Stop the Key Agent" on page 460

Configure Reflection to Authenticate Using the Key Agent

If your Reflection application supports Secure Shell connections, you can use this procedure to configure it to authenticate using the Key Agent.

To configure Reflection to authenticate using a key in the agent

1 Add a private key (page 454) to the Key Agent, or import a certificate (page 456).

2 Configure the host:

If you are authenticating	Do this
Using keys	Upload the public key (page 455).
Using certificates	Install the CA certificate on the host and configure the host for user authentication with certificates. (Refer to your Secure Shell server documentation for more information.)

3 Launch your Reflection application that supports Secure Shell connections and open the **Reflection Secure Shell Settings** dialog box.

4 From side menu, select the **User Authentication** section, make sure that **Public Key** is selected. If you want to ensure that only public key authentication is used, clear the other options.

5 From the side menu, select **User Keys**. In the Key Agent section of the dialog select **Allow Agent Forwarding**.The keys and certificates in the Reflection Key Agent are included in the list of available keys.

6 In the **User Keys** list view, select the key(s) or certificate(s) you want to use to authenticate to the currently specified host, and then click **OK**.

NOTE

- ◆ Secure Shell settings are saved in your Secure Shell configuration file and apply to a specific SSH configuration scheme. (If you don't specify a scheme, settings apply to all connections to the current host.)

- ◆ You do not need to repeat the client configuration steps for new connections using the same SSH configuration scheme (or host name).

Managing Keys and Certificates

Use these procedures to manage keys and certificates in the Reflection Key Agent.

In this Section

- ◆ "Add Keys to the Key Agent" on page 454
- ◆ "Upload Keys to the Server" on page 455
- ◆ "Import Keys to the Key Agent" on page 456
- ◆ "Import Certificates to the Key Agent" on page 456
- ◆ "Export Public Keys" on page 456
- ◆ "Allow Adding Keys Remotely" on page 457
- ◆ "Allow Deleting Keys Remotely" on page 457
- ◆ "Confirm Remote Private Key Operations" on page 457
- ◆ "Limiting RSA Signatures to SHA1" on page 458
- ◆ "Generate Key Dialog Box" on page 458

Add Keys to the Key Agent

You can add keys to the Key Agent by generating keys using the Key Agent, or by importing keys that you have created using Reflection or other applications. Keys you create using the Key Agent are stored by the agent in encrypted form and can only be accessed by using the Key Agent. Keys you create using the Reflection **Secure Shell Settings** dialog box are stored in your <personal documents folder>\Micro Focus\Reflection\.ssh folder. When you import a key into the Key Agent, the imported key is stored within the agent in encrypted form, and the original key also remains available unless you delete it.

To generate a new key pair using the Key agent

1 Start and unlock (page 452) the Key Agent.

2 Click **Generate Key**.

3 Specify a key name, key type, and key length, and then click **OK**.

To generate a new key pair using Reflection

1 Open the **Reflection Secure Shell Settings** dialog box

2 From the side menu, select **User Keys**. Select the **generate** icon (+).

3 Specify a key name, key type, and key length. (Use the **Browse** button to specify a non-default name or location for the key.)

4 Either specify a passphrase, or select **No passphrase**.

5 Click **Create**.

To import a private key into the Key Agent

1 the Key Agent.

2 From the **File** menu, click **Import Private Key**.

3 Select the key you want to add. The default location for keys you create using Reflection is:

personal_documents_folder\Micro Focus\Reflection\.ssh

For example:

C:\users\joe\documents\Micro Focus\Reflection\.ssh

The Agent opens this folder by default when you click **Import Private Key**. Each key pair includes two files: one with a *.pub extension; and one with no file extension. The private key is the file with no extension.

4 If the key is protected by a passphrase, you must enter the phrase correctly before you can import the key.

After you import the key, it is protected by the Key Agent passphrase. The original key and passphrase are not changed.

Related Topics

Upload Keys to the Server

Secure Shell key authentication uses a public/private key pair. The public key must be added to the authorized keys on a host before you can authenticate to that host using the key pair. You can use the Key Agent to make the upload process easy. The agent automatically determines what kind of Secure Shell server is running on the host you specify, exports your public key using the correct key type for that host, and installs it (using SFTP) to the correct location for the user you specify.

The public key is transferred using the secure SFTP protocol. You will need the ability to use password authentication in order to upload the public key.

To upload the public key to the server

1 the Key Agent.

2 Select the key you want to use for authentication to the server, and click **Upload**.

3 Enter the name of the host to which you are uploading the key. (In most cases you can leave **SSH config scheme** blank. The Key Agent makes a Secure Shell connection to the host in order to upload the key. The SSH configuration scheme you specify determines which SSH settings are used for this connection.) Click **OK**.

4 When prompted, enter the name and password of the user who will authenticate to the host using the key.

After the secure connection to the host has been established, a dialog box appears displaying information about where on the host Reflection will upload this key. In most cases you do not need to change these settings. See the notes below for more information.

NOTE

◆ **Upload** is not available if the Key Agent is locked.

◆ The **Upload Public Key** dialog box displays information about the transfer. Click **OK** to close this dialog box.

◆ Keys uploaded to hosts running Reflection for Secure IT, F-Secure, and SSH Communications (SSH Tectia) servers are exported to SECSH format. By default these are installed to the user's `.ssh2` directory and an appropriate `KEY` entry is made in the `authorization` file. If this file did not previously exist, it is created and given appropriate file permissions.

◆ Keys uploaded to hosts running OpenSSH servers are exported using OPENSSH format. By default they are added to the `authorized_keys` file located in the user's `.ssh2` directory. If this file did not previously exist, it is created and given appropriate file permissions.

Import Keys to the Key Agent

◆ Choose **File** > **Import Private Key**.

NOTE: **Import Private Key** is not available if the Key Agent is locked.

After the import, the original key remains in its original location. A copy is added in encrypted form to the agent. If the imported key is encrypted with a passphrase, you are prompted to enter it.

Related Topics

◆ "Configure Reflection to Authenticate Using the Key Agent" on page 453

Import Certificates to the Key Agent

1 Start and unlock (page 452) the Key Agent.

2 From the **File** menu, select **Import Certificate from <store>**.

All certificates currently available in the certificate store you selected are displayed.

3 Select the certificate you want to import, and then click **OK**.

Export Public Keys

You can export plain text public keys from keys stored in the Reflection Key agent.

To export a plain text public key

1 Select the public key that you want to export.

2 Choose **File** > **Export Public Key**.

The agent exports the public key for the currently selected key.

> **NOTE:** The Key Agent exports keys using the Reflection native format by default.

3 (Optional) Select **Save in OpenSSH format** to save to the format used by OpenSSH servers.

NOTE

- If you want to upload a public key to a Secure Shell server, you can use the **Upload** button to do this in a single step; you do not need to export the public key first. The upload utility automatically determines the correct key format for the server you specify.
- **Export Public Key** is not available if the Key Agent is locked.

Allow Adding Keys Remotely

You can configure Reflection to add keys to the Reflection Key Agent automatically when you add them to a remote host.

To enable this feature

1 From the Key Agent **Options** menu, select **Allow Adding Keys Remotely**.

2 Open the **Reflection Secure Shell Settings** dialog box.

3 From the side menu, select **User Keys**, select **Allow agent forwarding**.

> **NOTE:** Agent forwarding must also be enabled on the host.

Allow Deleting Keys Remotely

You can configure Reflection to remove keys from the Reflection Key Agent automatically when you delete them from a remote host.

To enable this feature

1 From the Key Agent **Options** menu, select **Allow Deleting Keys Remotely**.

2 Open the **Reflection Secure Shell Settings** dialog box.

3 From the side menu, select **User Keys**, select **Allow agent forwarding**.

> **NOTE:** Agent forwarding must also be enabled on the host.

Confirm Remote Private Key Operations

You can configure whether to have the Key Agent confirm whenever a connection is made using a key in the agent.

To configure remote private key operations

• From the Key Agent **Options** menu, select or clear **Confirm Remote Private Key Operations**.

The Key Agent displays a confirmation dialog box whenever a connection is made using a key in the agent; when cleared, a key exchange occurs in the background, and connections are made with no prompting.

Limiting RSA Signatures to SHA1

For compatibility with older servers, you can configure the agent to only include RSA signatures that use SHA1 when responding to the Agent Identities Request.

NOTE: Agent forwarding to some servers may not be supported when this option is unchecked because of the length of the reply to the list request.

Generate Key Dialog Box

Getting there

1 Start the Reflection Key Agent (page 452).

2 Click **Generate Key**.

Secure Shell key authentication uses a public/private key pair. From this dialog box, you can create a new key pair and add it to the Key Agent. When you generate keys using the Key Agent, the private key is always kept in encrypted form for use by the Reflection Key Agent only.

The options are:

Name	Enter a name to identify this key.
Type	Specifies the algorithm used for key generation.
Length	Specifies the key size. Up to a point, a larger key size improves security. Increasing key size slows down the initial connection, but has no effect on the speed of encryption or decryption of the data stream after a successful connection has been made. The length of key you should use depends on many factors, including: the key type, the lifetime of the key, the value of the data being protected, the resources available to a potential attacker, and the size of the symmetric key you use in conjunction with this asymmetric key. To ensure the best choice for your needs, we recommend that you contact your security officer.

NOTE: Only public keys can be exported from the agent.

Working with the Key Agent

In this Section

• "Key Agent Passphrase" on page 459

• "Change Passphrase Dialog Box" on page 459

• "Lock or Unlock the Key Agent" on page 459

Key Agent Passphrase

You are prompted for a passphrase (page 459) the first time you use the Key Agent. Use this phrase whenever you need to unlock the agent.

A passphrase is similar to a password, except it can be a phrase with a series of words, punctuation, numbers, white space, or any string of characters you want. Passphrases improve security by limiting access to secure objects, such as private keys and the Reflection Key Agent.

Good passphrases are 10-30 characters long, are not simple sentences or otherwise easily guessable, and contain a mix of upper and lower case letters, numbers, and non-alphanumeric characters. The passphrase is case-sensitive.

NOTE

- Use **Change Passphrase** (page 459) to change your passphrase.
- There is no way to recover a lost passphrase. If the passphrase is lost or forgotten, you can reset the Key Agent using the **Reset** button in the **Change Passphrase** dialog box. When you do this you lose all the keys stored in the agent.

Change Passphrase Dialog Box

Getting there

1 Start the Reflection Key Agent (page 452).

2 Click **Change Passphrase**.

Use **Change Passphrase** to change the passphrase (page 459) you use to unlock the Key Agent.

Reset	There is no way to recover a lost passphrase. If the passphrase is lost or forgotten, you can use the **Reset** button to clear the current passphrase.
	NOTE: Using **Reset** will also destroy all the keys in the agent. If you added keys to the agent using Import, the original keys remain available after a reset, protected by their original passphrase.

Lock or Unlock the Key Agent

When the Agent is locked, you cannot add, modify, or use the Key Agent keys. If you attempt to connect to a host that is configured to use keys in the agent, you will be prompted for your passphrase (page 459).

When you unlock the agent, it remains unlocked until you lock it, shut down the agent, or log off Windows.

To lock the Key Agent

- From Reflection Key Agent, choose the **Lock** button.

To unlock the Key Agent

* From Reflection Key Agent, choose the **Unlock** button, and then enter the passphrase (page 459).

-or-

1 Connect to a host that is configured to authenticate using the Key Agent.

2 When prompted, enter the correct passphrase.

NOTE: There is no way to recover a lost passphrase. If the passphrase is lost or forgotten, you can reset the Key Agent using the **Reset** button in the **Change Passphrase** dialog box. When you do this you lose all the keys stored in the agent.

Hide and View the Key Agent

To hide the Key Agent window

* From the **File** menu, click **Hide**. The key agent continues to run in the background.

NOTE: Whenever the Key Agent is running, the Key Agent icon is visible in the Windows system tray.

To view the Key Agent window after it has been hidden

* Right-click the Key Agent icon, and select **Open Reflection Key Agent**.

Stop the Key Agent

Do one of the following:

* From the Key Agent **File** menu, click **Exit**.
* Right-click the Key Agent icon in the system tray, then click **Exit**.
* Log off Windows.

View the Key Agent Log File

From the **View** menu, choose **Log**

Certificate Authentication in Secure Shell Sessions

In this Section

* "PKI and Certificates" on page 461
* "Configure Client Authentication using Certificates" on page 461

PKI and Certificates

A Public Key Infrastructure (PKI) is a system that helps facilitate secure communications through the use of digital certificates. Reflection supports the use of a PKI for both host and user authentication.

Like public key authentication, certificate authentication uses public/private key pairs to verify the host identity. However, with certificate authentication, public keys are contained within digital certificates (page 897), and in this case, two key pairs are used. For example, for server authentication, the host holds one private key and the CA holds a second. The host obtains a certificate from the CA. This certificate contains identifying information about the host, a copy of the host public key, and a "digital signature" on page 897 created using the CA's private key. This certificate is sent to the client during the authentication process. To verify the integrity of the information coming from the host, the client must have a copy of the CA's public key, which is contained in the CA root certificate. There is no need for the client to have a copy of the host public key.

Certificate authentication solves some of the problems presented by public key authentication. For example, for host public key authentication, the system administrator must either distribute host keys for every server to each client's known hosts store, or count on client users to confirm the host identity correctly when they connect to an unknown host. When certificates are used for host authentication, a single CA root certificate can be used to authenticate multiple hosts. In many cases the required certificate is already available in the Windows certificate store.

Similarly, when public keys are used for client authentication, each client public key must be uploaded to the server and the server must be configured to recognize that key. When certificate authentication is used, a single CA root certificate can be used to authenticate multiple client users.

Related Topics

- "Certificate Authentication (PKI)" on page 520
- "Reflection Certificate Manager" on page 528

Configure Client Authentication using Certificates

Digital certificates (page 897) can be used for either host and/or client "authentication" on page 897 in Secure Shell client sessions. Certificates are not required and are not used by default. This topic describes how to configure the Reflection client for certificate authentication. For information about how to configure the Secure Shell server, consult the server documentation.

To configure certificate authentication on the client

1 Obtain a file that contains your personal certificate and an associated private key (such as a *.pfx or *.p12 file). (You can obtain certificates from a certification authority.)

2 Use this file to import the certificate into the personal tab of either the "Reflection Certificate Manager" on page 528 or the Windows certificate store.

3 From Reflection, open the **Reflection Secure Shell Settings (page 469)** dialog box.

4 From the **General** tab, make sure that **Public Key** is selected under **User Authentication** (the default).

5 From the **User Keys** tab, locate the certificate you want to use from the list of available keys, and then to enable its use, select it in the **Use** column.

Related Topics

◆ "Certificate Authentication (PKI)" on page 520

Port Forwarding

Port forwarding, also known as tunneling, provides a way to redirect communications through the Secure Shell channel of an active session. When port forwarding is configured, all data sent to a specified port is redirected through the secure channel. You can configure either local or remote port forwarding. The terms "local" and "remote" refer to redirected port locations with reference to the Secure Shell client. Reflection supports local port forwarding for both TCP and FTP communications. Remote port forwarding is supported for TCP communications only.

Terminology

Port forwarding involves two sets of client and server applications — the Secure Shell client and server, and the client/server pair whose data is being forwarded. In this guide, the following terms are used as defined below in reference to port forwarding:

Term	Definition
Secure Shell server	The Reflection server daemon.
Secure Shell server host	The computer on which the Secure Shell server runs.
Secure Shell client	The Reflection client application.
Secure Shell client host	The computer on which the Secure Shell client runs.
Application client	The client program of the client/server pair whose data you want to forward. For example, this might be a mail client or Web browser.
Application client host	The computer on which the application client runs. This is often either the Secure Shell server host or the Secure Shell client host, but it can also be a third host.
Application server	The server program that communicates with your application client, such as a mail server or Web server.
Application server host	The computer on which the server application runs. This can be either the Secure Shell server host or the Secure Shell client host, or it can also be a third host.

In this Section

◆ "Local Port Forwarding" on page 463
◆ "Remote Port Forwarding" on page 465
◆ "Forward TCP communications" on page 466
◆ "Configure Multi-hop Secure Shell Sessions" on page 468

Local Port Forwarding

Use local port forwarding to forward data securely from an application client running on the same computer as the Secure Shell client. When you configure local port forwarding, you designate an arbitrary local port to use for forwarding data, and a destination host and port to receive the data.

Local port forwarding works as follows:

1. When the Secure Shell connection is established, the Secure Shell client opens a listening "socket" on page 900 on the local computer (the one running the Secure Shell client) using the designated local port. In most cases, this socket is available only to applications running on the Secure Shell client host.

   The gateway ports setting controls whether locally forwarded ports are available to remote applications. By default this setting is not enabled, and the client uses the loopback address ("localhost" or 127.0.0.1) when it opens a socket for local port forwarding. This prevents applications running on other computers from connecting to the forwarded port. When you enable gateway ports, a remote application client can open a socket using the Secure Shell client's Ethernet address (such as an IP address, a URL, or a DNS name). For example, a Secure Shell client running on acme.com might be configured to forward port 8088. When gateway ports are not enabled, the forwarded socket is localhost:8088. When gateway ports are enabled, the forwarded socket is acme.com:8088.

   CAUTION: Enabling gateway ports reduces the security of your client host, network, and connection because it allows remote applications to use the forwarded port on your system without authenticating.

2. An application client is configured to connect to the forwarded port (rather than directly to the application server host and port). When that client establishes a connection, all data is sent to the listening port, and then redirected to the Secure Shell client.

3. The Secure Shell client encrypts the data and sends it securely through the Secure Shell channel to the Secure Shell server.

4. The Secure Shell server receives the data, decrypts it, and redirects it to the destination host and port used by the application server.

   NOTE: If the final destination host and port are not on the Secure Shell server host, data is sent in the clear between the Secure Shell host and the application server host.

5. The return data from the application server is directed to the Secure Shell server, which encrypts it and sends it securely to the Secure Shell client through the SSH tunnel. The Secure Shell client decrypts the data and redirects it to the original application client.

The general command-line syntax for local port forwarding is:

```
ssh -L
    listening_port:
    app_
    host:
    hostport user@
    sshserver
```

The diagrams that follow illustrate two ways to use this.
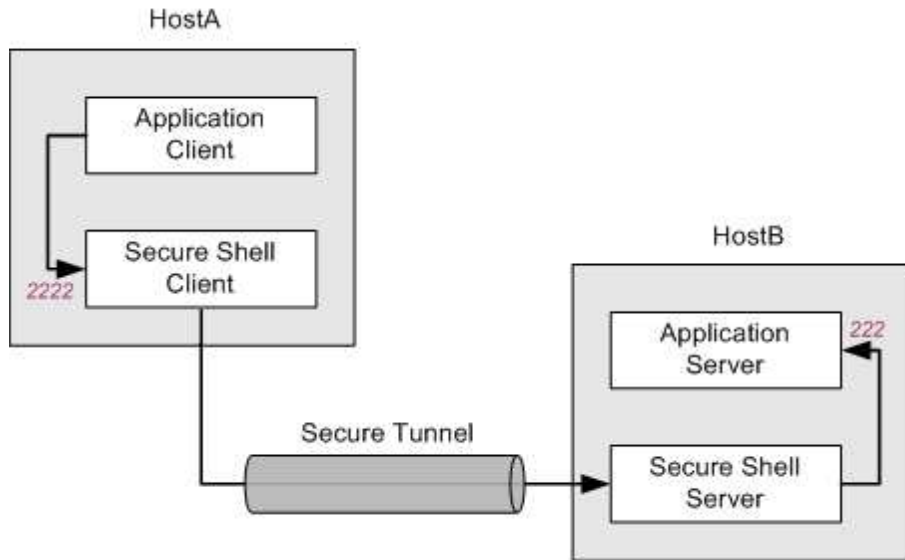
In the configuration shown above, the application client and the Secure Shell client both run on HostA. The Secure Shell server and application server both run on HostB. All data sent to port 2222 on HostA is forwarded to port 222 on HostB. In this arrangement, all data in transit is securely encrypted. The following command (in which `localhost` identifies the loopback address on HostB) configures this:

```
ssh -L 2222:localhost:222 user@HostB
```

The following diagram illustrates local port forwarding to a third host. In this configuration, the application server runs on a different host than the Secure Shell server. All data sent to port 2222 on HostA is forwarded to port 222 on HostC.
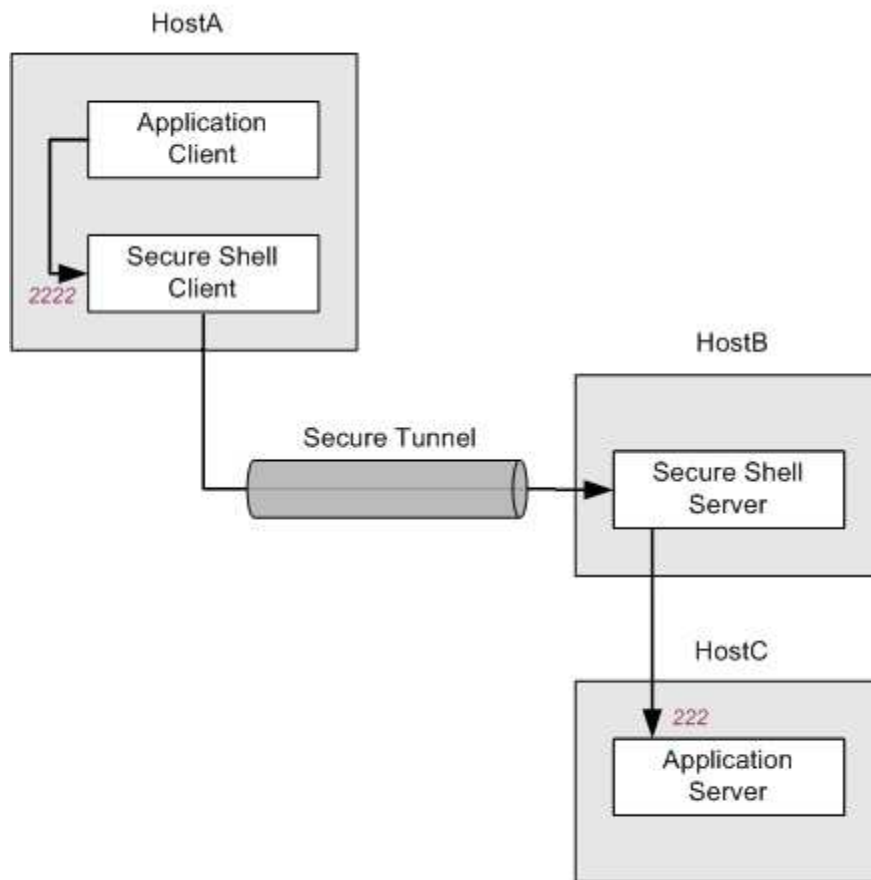
The following command configures this:

```
ssh -L 2222:HostC:222 user@HostB
```

NOTE: Data sent between HostB and HostC is not encrypted.

Remote Port Forwarding

Use remote port forwarding to forward data securely from an application client running on the Secure Shell server host. When you configure remote port forwarding, you designate an arbitrary remote port to use for forwarding data and a destination host and port to receive the data.

Remote port forwarding works as follows:

1. When the Secure Shell connection is established, the Secure Shell server opens a listening "socket" on page 900 on the Secure Shell server host using the specified listening port.

2. A client application running on the Secure Shell server host is configured to connect to the listening port (rather than directly to the application server host and port). When that client establishes a connection, all data is sent to the listening port, and then redirected to the Secure Shell server.

3. The Secure Shell server encrypts the data and sends it securely through the SSH tunnel to the Secure Shell client.

4. The Secure Shell client receives data, decrypts it, and redirects it to the destination host and port (on the Secure Shell client host) that is used by the server application.

5. The return data from the server application is directed to the Secure Shell client, which encrypts it and sends it securely to the Secure Shell server through the SSH tunnel. The Secure Shell server decrypts the data and redirects it to the original client application.

The general command-line syntax for remote port forwarding is:

```
ssh -R
    listening_
    port:
    app_
    host:
    hostport user@
    sshserver
```

The diagram that follows illustrates one possible remote port forwarding configuration.
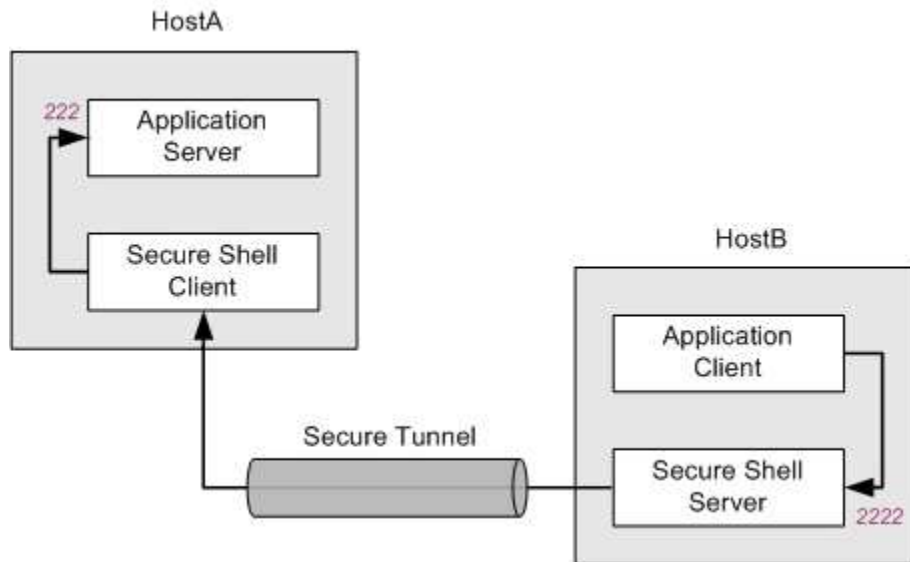
The application server and the Secure Shell client run on HostA. The Secure Shell server and application client both run on HostB. All data sent to port 2222 on HostB is forwarded to port 222 on HostA. In this arrangement, all data in transit is securely encrypted. The following command configures this.

```
ssh -R 2222:localhost:222 user@HostB
```

Forward TCP communications

Use this procedure to encrypt TCP communications that would otherwise be sent in the clear between an application client and server. (Examples given in parentheses configure the Reflection client to send data securely between a Web browser on the computer running Reflection, and a remote Web server.)

To forward TCP communications

1 Open the Reflection client and configure it to connect to your Secure Shell server host (for example, MySSHserver.com).

2 Open the **Reflection Secure Shell Settings** dialog box (page 483). Go to the **Tunneling**tab.

3 Under **Local Forwarding**, click **Add**.

4 For **Forward local port**, specify any available local port. You can typically enter any value greater than 1024 (for example, 8080). Ports with values less than or equal to 1024 are, by convention, reserved for services and may not be available.

5 Under **Destination Host**, specify the **Name**of the application server host (for example, WebServer.Acme.com).

NOTE: If this server host is different than your Secure Shell Server host, communications between the Secure Shell server and the designated server are not encrypted. If the designated server runs on the same remote computer as the Secure Shell server host, you can specify the value **localhost**(or the IP equivalent, `127.0.0.1`). In this case, all communications are encrypted.

6 For **Port**, specify the port used by the application server (for example, 80 for a Web server or 110 for a mail server).

NOTE: Although the next two steps are not required, completing them configures Reflection to launch the application client automatically after the Secure Shell tunnel is established.

7 (Optional) Under **Application to Launch**, specify the name of the client application whose data you want to forward through the tunnel (for example, `iexplore.exe`). For applications that are not in your system path, you must include full path information. You can use the **Browse** button to locate the executable file and full path information will be included.

8 (Optional) Under **Arguments**, specify any command line arguments you want to use with this application. (For example, the browser can be set to connect to the redirected port 8080 using `http:\\localhost:8080`.) You may also need to run your application client to configure it to connect to the specified port.

9 Click **OK** to close the open dialog boxes.

NOTE: The **Local Port Forwarding** dialog box **OK** button is not available until all required information has been entered.

10 Connect to the Secure Shell host.

After the Secure Shell connection is established, the application you specified in step 7 will launch. If it is correctly configured to connect to the forwarded local port (8080 in this example), data will be redirected from this port to the server application. The client will run exactly as if it had been configured to connect directly to that server.

Related Topics

◆ "Forward FTP communications" on page 784

Configure Multi-hop Secure Shell Sessions

Use multi-hop connections when you need to establish secure connections through a series of Secure Shell servers. This is useful if your network configuration doesn't allow direct access to a remote server, but does allow access via intermediate servers. The diagram represents such a series. The Windows workstation needs secure access to ServerC, but cannot connect directly to either ServerB or ServerC. ServerA can connect to ServerB which, in turn, can connect to ServerC.

Windows workstation ➡ ServerA ➡ ServerB ➡ ServerC

When you configure a multi-hop list, Reflection creates a secure end-to-end connection by establishing a series of secure tunnels. Each tunnel is established within an existing tunnel, and goes one step further along the chain.

The last server in the chain is the host you specified when you set up your initial Secure Shell connection. Add the other servers in order (top to bottom starting from the client side) to your multi-hop server list. The following procedure describes how to do this.

To configure multi-hop sessions

1 Configure a Reflection Secure Shell session to your final destination host (ServerC in this example).

2 Open the **Reflection Secure Shell Settings** dialog box (page 483).

3 Click the **Multi-hop** tab.

4 Click **Add**, and then configure the connection to the first multi-hop server in your configuration (ServerA in this example).

   4a For **Host name** specify the destination host for this hop (ServerA in this example).

   4b (Optional) Specify a value for **User name** if this host requires a user name that's not the same as the user you specified for your original host connection. (In this example, you would need to specify a user name if ServerA and ServerC require different user names.)

   4c (Optional) Modify the **Port**value if your host doesn't use port 22 for Secure Shell connections.

   4d (Optional) Click Configure, or specify an SSH configuration scheme (page 485) to use non-default Secure Shell settings for this connection.

   4e Click **OK**.

5 Click **Add** again to configure connections to any additional multi-hop servers (ServerB in this example).

NOTE: If you are using this connection to tunnel data for another application (such as a browser or mail client), use the **Tunneling (page 481)** tab to configure that port forwarding. For example, if your mail server runs on ServerC, after configuring this multihop, you can create a new local port forward as follows: for **Local port to forward**, specify any unused port (for example 1110), for the remote host **Name,**enter **localhost**("localhost" in this context identifies the last server in the series-ServerC in the example above), and set the **Port**value equal to your mail server port (usually 110). When the Reflection multihop tunnel is established, you will be able to access the mail server securely by configuring your local mail client to connect to `localhost:1110`.

Reflection Secure Shell Settings Dialog Box

Use the **Reflection Secure Shell Settings** dialog box to manage Secure Shell settings and keys.

NOTE

- The settings you configure in this dialog box are saved to the Secure Shell configuration file (page 484). You can also configure Secure Shell settings by editing this file manually in any text editor.

- Within the configuration file, these settings are saved for the currently specified SSH configuration scheme (page 485).

- "General (Secure Shell Settings)" on page 469
- "Security Proxy (Secure Shell Settings)" on page 470
- "User Authentication (Secure Shell Settings)" on page 472
- "User Keys (Secure Shell Settings)" on page 472
- "User Key Generation Dialog Box" on page 474
- "GSSAPI (Secure Shell Settings)" on page 475
- "Encryption (Secure Shell Settings)" on page 475
- "Host Data (Secure Shell Settings)" on page 476
- "Host Authentication (Secure Shell Settings)" on page 477
- "Multi-hop (Secure Shell Settings)" on page 478
- "PKI (Secure Shell Settings)" on page 479
- "Proxy (Secure Shell Settings)" on page 480
- "Tunneling (Secure Shell Settings)" on page 481

General (Secure Shell Settings)

The options are:

Port number	Specifies the port to connect to on the server. The default is 22, which is the standard port for Secure Shell connections.
Enable server Keep Alive	When **Enable server Keep Alive** is selected, Reflection sends NOOP messages to the server through the secure tunnel at the specified interval. Use this setting to maintain the connection to the server. Use **Interval** to specify how frequently server alive messages are sent. If this is setting is not enabled, the Secure Shell connection will not terminate if the server dies or the network connection is lost. This setting can also be used to keep connections that only forward TCP sessions from being timed out by the server, as the server may timeout these connections because it detects no SSH traffic.
	The Secure Shell **Enable server Keep Alive** setting is not related to the TCP keep alive setting that can be set in the Windows registry to keep all TCP/IP connections from being timed out by a firewall. To change the TCP/IP keep alive behavior, you need to edit the Windows registry.

Enable compression	When **Enable compression** is selected, the client requests compression of all data. Compression is desirable on modem lines and other slow connections, but will only slow down response rate on fast networks.
Reuse existing connection if available	By default, multiple sessions to the same host reuse (page 443) the original Secure Shell connection, and therefore don't require re-authentication. If you clear **Reuse existing connection if available**, Reflection establishes a new connection for each session, which means that each new connection repeats the authentication process.
Logging Level	Determines how much information is written to the Secure Shell log file.

NOTE

◆ The settings you configure in this dialog box are saved to the Secure Shell configuration file (page 484). You can also configure Secure Shell settings by editing this file manually in any text editor.

◆ Within the configuration file, these settings are saved for the currently specified SSH configuration scheme (page 485).

Security Proxy (Secure Shell Settings)

Security Proxy and its related settings are visible for sessions that are managed by the Host Access Management and Security Server (MSS). Sessions that are set up on this server can be configured to connect to your host via the Security Proxy included in the centralized management server. You can use this Security Proxy to configure secure connections even if your host is not running an SSL/TLS-enabled Telnet server.

NOTE

◆ When the Security Proxy is used, the connection between the client and the Security Proxy server is secured and encrypted using the SSL/TLS protocol.

◆ If you configure sessions that connect through the Security Proxy with authorization enabled, users must authenticate to the centralized management server before they can connect using these sessions. This can be accomplished by the default login prompt or by setting up the centralized management server for Single Sign-On.

Use Security Proxy	Configure this session to use the Security Proxy for the server connection. Enable this option to access the Security Proxy configuration options below.
Proxy name	Select the proxy server name from the drop-down list, which shows available servers.
Proxy port	Select the proxy server port from the drop-down list.
Proxy cipher suites	A read-only list of cipher suites supported by this proxy host and port. This list is only visible when the product is launched from the centralized management server.
Destination host	Enter the destination host name.
Destination port	Enter the destination port.

Security proxy SSL/TLS settings

SSL/TLS version	Specifies which SSL or TLS version to use.

Encryption Strength

Encryption Strength	Specify the desired level of encryption for SSL/TLS connections. The connection will fail if this level cannot be provided.
	If you select **Recommended ciphers**, the FTP Client will negotiate with the host system to choose the strongest encryption level supported by both the host and the client. This new setting will contain the recommended encryption level from Micro Focus, and will change periodically.
	If you are running in FIPS mode and select **Recommended Ciphers**, the FTP Client will negotiate using only FIPS compliant encryption levels.
	If you select **Custom ciphers**, you will be prompted to select from a list of available ciphers in the **Custom Ciphers** list view.
	NOTE: Session files from previous versions of Reflection that use default, 168, 128 or 256 bit Encryption Strength will be imported as **Custom Ciphers** and maintain the list that was used in prior versions for those settings options.
Retrieve and validate certificate chain	Specifies whether certificates presented for host authentication are checked to determine if they are valid and signed by a trusted CA.
	CAUTION: Disabling this option can make connections vulnerable to man-in-the-middle attacks, which could compromise the security of the connection.

Security proxy client authentication

Automatically select client certificate	When enabled, the first qualifying certificate is presented to the server.
Prompt for certificate	When enabled, the user will be prompted to select a particular certificate for client authentication.
Use selected certificate for authentication	Select to specify a particular certificate for client authentication.

User Authentication (Secure Shell Settings)

Use the **User Authentication** section of the **Secure Shell Settings** dialog box to configure your authentication preferences. You must select at least one authentication method.

Select from the following User Authentication Options

- GSSAPI
- Public Key
- Keyboard Interactive
- Password

NOTE: Changes you make in this dialog box are saved to the currently specified SSH configuration scheme (page 485) when you click **OK**.

User Keys (Secure Shell Settings)

Use the User Keys section under the User Authentication option of the Secure Shell Settings dialog box to create and manage the keys that authenticate your client session to the host.

Reflection maintains a list of available user keys. To specify which key or keys you want Reflection to use for authentication to the current host, select one or more check boxes in the **Use** column (or enable **Use all keys for authenticating to the host**).

The list of keys includes:

- Keys you have created using the **User Key Generation** (page 474) dialog box.
- Keys you have added using the **Import** button.
- Keys you have copied manually to the Secure Shell folder.
- Keys and certificates in the Key Agent.
- User and Authentication Agent keys copied during migration of F-Secure settings.
- Certificates in the Windows Certificate Manager in your personal store.
- Certificates in the Reflection Certificate Manager in your personal store.

The following key management tools are also available:

User keys

Select keys to use for authenticating to the host:

Generate (+)
Opens the User Key Generation (page 474) dialog box, which you can use to configure a public/private key pair for user key authentication.

View (👁)
Displays the contents of the selected key or certificate.

Upload (⬆)
Upload a public key to the currently specified host. The utility automatically detects the host type and uploads the key by default using appropriate settings for this host. After the secure connection to the host has been established, a dialog box appears, displaying information about where on the host to upload the key. In most cases you do not need to change these settings.

If the host or key type determined by the utility is incorrect, you can configure host-specific values for key uploads by setting the `ServerKeyFormat` and `ServerStyle` keywords in the Secure Shell configuration file (page 486).

The public key is transferred using the secure SFTP protocol. You will need the ability to use password authentication (or another authentication method) in order to upload the public key. Once the public key is successfully uploaded, you may disable other authentication methods.

Import (📥)
Add a private key to the list of available keys. You can use this feature to provide easy access to keys created using other applications. Importing a key copies it to the Secure Shell folder.

Export (📤)
Export a public key or public/private key pair.

Delete (🗑)
Deletes the selected key.

Change Passphrase (⌨)
Change the passphrase used to protect the selected key.

Add to Key Agent (🔑)
Adds the selected key to the Key Agent. If you have not yet started the Key Agent for the first time, or if the Key Agent is locked, you will be prompted to enter the Key Agent passphrase. In addition, you will be prompted to enter the private key's passphrase before the key can be added to the agent.

Authentication options

Use all keys for authenticating to the host	When this option is selected, the client attempts to authenticate with all the listed keys, regardless of whether or not the Use checkbox is selected.
Prefer SSH key signature over certificate signature	This setting determines the order in which the client presents certificate signature types to the server during public key authentication. When this setting is selected (the default), the client sends the key using a standard ssh key signature first (ssh-rsa or ssh-dss). If that fails, the client tries again using a certificate signature (x509-sign-rsa or x509-sign-dss).
	When this option is cleared, the client presents the certificate signature first. This can be useful in situations where the certificate key type is required and the server doesn't allow the client to attempt a second authentication using the same key with a different signature type.

Key agent

Allow Agent Forwarding	Enables forwarding of the Key Agent connection. Agent forwarding should be enabled with caution. Users with the ability to bypass file permissions on the remote host (for the agent's Unix-domain socket) can access the local agent through the forwarded connection. Attackers cannot obtain key material from the agent, however they can perform operations on the keys that enable them to authenticate using the identities loaded into the agent.
Add key used for authenticating to host to key agent	This setting is available when **Allow agent forwarding** is enabled. When it is selected and public key authentication to the server is successful, the key or certificate that was used for authentication is automatically added to the Key Agent. This key is not saved in the Key Agent, but remains available as long as the Key Agent is running.
Launch Key Agent	Launches the Key Agent.

User Key Generation Dialog Box

Getting there

1 Open the **Reflection Secure Shell Settings** dialog box.

2 Click **User Keys**, located under the **User Authentication** section.

3 Click the **Generate Key** icon (+).

Use this dialog box to configure a public/private key pair for user key authentication.

The options are:

Key Type	Specifies the algorithm used for key generation.

Key Length	Specifies the key size. Up to a point, a larger key size improves security. Increasing key size slows down the initial connection, but has no effect on the speed of encryption or decryption of the data stream after a successful connection has been made. The length of key you should use depends on many factors, including: the key type, the lifetime of the key, the value of the data being protected, the resources available to a potential attacker, and the size of the symmetric key you use in conjunction with this asymmetric key. To ensure the best choice for your needs, we recommend that you contact your security officer.
No passphrase	Select this check box if you want to connect without being prompted for a passphrase. Note: If you select **No passphrase**, the private key saved to your computer is unencrypted.
Passphrase	Specify a passphrase that will be required when you connect with this key. Note: If you don't want to use a passphrase, you must select the **No passphrase** setting.
Verify	Retype the passphrase here for confirmation.
OK	Opens a browse dialog box that allows you to select a name and location for the private key. (The default name identifies the key type, size, and the client host name.) The public key is saved to the same location using the private key name with an added *.pub file extension.

GSSAPI (Secure Shell Settings)

Use the **GSSAPI** section under the **User Authentication** option of the **Secure Shell Settings** dialog box to specify settings for GSSAPI authentication. Items on this tab are available only if **GSSAPI** is selected in the **User Authentication** list on the **General** (page 469) tab.

The options are:

Delegate credentials	Specifies whether GSSAPI forwards your ticket granting ticket (TGT) to the host.
Use default service principal name	Specifies the name used to send a request for a service ticket to the Key Distribution Center (KDC). The host name value is the name of the Secure Shell server to which you are connecting. The realm value depends on which GSSAPI provider you have selected.

Encryption (Secure Shell Settings)

Use the **Encryption** section of the **Secure Shell Settings** dialog box to specify what ciphers the Secure Shell connection should use. Different options are available depending on which Secure Shell protocol is used for the connection.

The options are:

Run in FIPS Mode	When Run in FIPS mode is selected, Reflection enforces the United States government Federal Information Processing Standard (FIPS) 140-2 for this connection. Options on the Encryption tab that do not meet this standard are not available when Run in FIPS mode is selected.

Cipher List	Use this list to specify the ciphers you want to allow for protocol 2 connections to the current host. When more than one cipher is selected, the Secure Shell client attempts to use ciphers in the order you specify, starting from the top. To change the order, select a cipher from the list, then click the up or down arrow. The cipher used for a given session is the first item in this list that is also supported by the server.
HMAC List	Specifies the HMAC (hashed message authentication code) methods you want to allow. This hash is used to verify the integrity of all data packets exchanged with the server. When more than one HMAC is selected, the Secure Shell client attempts to negotiate an HMAC with the server in the order you specify, starting from the top. To change the order, select an HMAC from the list, then click the up or down arrow.
Key Exchange Algorithms	Specifies which key exchange algorithms the client supports, and the order of preference.
	In some cases, you may need to change the order of the key exchange algorithms to put DH Group14 SHA1 ahead of the other values. This is required if you want use the hmac-sha512 MAC, or if you see the following error during key exchange: "fatal: dh_gen_key: group too small: 1024 (2*need 1024)".
	Two additional encryption algorithms (gss-group1-sha1-*) are supported, but do not appear in the list of available key exchange algorithms. These two algorithms are automatically proposed by the client when you enable GSSAPI from the **General (page 469)** tab (under **User Authentication**).

NOTE

- The settings you configure in this dialog box are saved to the Secure Shell configuration file (page 484). You can also configure Secure Shell settings by editing this file manually in any text editor.

- Within the configuration file, these settings are saved for the currently specified SSH configuration scheme (page 485).

Host Data (Secure Shell Settings)

Use the **Host Data** section to set environment variables and run commands on the server.

The options are:

Environment Variables

Add (+)	Opens the **New Environment Variable** dialog box, from which you can specify a new variable and value.
Modify (✎)	Edit the selected variable.
Delete (✕)	Delete the selected variable.

Remote Command

Remote Command	Specifies one or more commands to run on the remote server. Use a semicolon (;) to separate multiple commands when connecting to a UNIX server. Use an ampersand (&) to separate commands when connecting to a Windows server. After a connection is established the server executes (or attempts to execute) the specified command(s), and then the session terminates. The server must be configured to allow commands received from the client to run.

The commands must be specified in the correct format for your server. For example, to capture a directory listing on a UNIX server, you might specify the following:

```
ls > list.txt
```

On a Windows server, the equivalent command would be one of the following, depending on how the Windows server is configured:

```
dir > list.txt
cmd /c dir > list.txt
```

Host Authentication (Secure Shell Settings)

Use the **Host Authentication** section to manage the keys that authenticate the host to your client session. You can use this tab to view the list of trusted hosts, add or delete host keys, and specify how you want Reflection to handle unknown hosts.

Host authentication enables the Secure Shell client to reliably confirm the identity of the Secure Shell server. This authentication is done using public key authentication. If the host public key has not previously been installed on the client, the first time you attempt to connect you see a message indicating that this is an unknown host. This message includes a fingerprint that identifies the host. To be sure that this is actually your host, you should contact the host system administrator who can confirm that this is the correct fingerprint. Until you know that the host is actually your host, you are at risk of a "man-in-the-middle" attack, in which another server poses as your host. If you select **Always** in response to this prompt, the host is added to the **Trusted Host Keys** list. To avoid the need to contact the host administrator, you can add host keys to the **Trusted Host Keys** list before the first connection.

The options are:

Enforce strict host key checking	Specifies how Reflection should handle host key checking when connecting to an unknown host. The options are:
	Ask User(default)
	Display the Host Key Authenticity confirmation dialog box when you connect to an unknown host.
	Yes (most secure)
	The connection is refused if the host is not a trusted host. Before you can connect, you must add the host key to your list of trusted host keys.
	No (least secure)
	No host key checking is done. The connection is made without displaying a confirmation dialog box. The host key is not added to the list of trusted keys.

Prefer SSH keys over certificates	Specifies the order of preference for host key algorithms. When this setting is unselected (the default), Reflection requests host certificates before host keys. When this setting is selected, Reflection requests host keys before host certificates.
	This setting is useful when the server is configured for both certificate and standard host key authentication. SSH protocol allows only one attempt to authenticate the host. If the host presents a certificate, and the client is not configured for host authentication using certificates, the connection fails. (This is different from user authentication, in which multiple authentication attempts are supported.)
Trusted Host Keys	Displays a list of trusted hosts for the current Windows user. You can modify the contents of this list using Import and Delete.
	By default, when you attempt a connection to a host that is not on this list, you are asked if you want to trust the new host key. If you select Always in response to this prompt, the host is added to the Trusted Host Keys list.
	Use the ⬑ **Import** button to import host keys. To delete from the Trusted Host Keys list hover over the desired host key and select the **Delete** button.
Global Host Keys (read only)	Displays a list of trusted host keys that are available to all users of the computer. Items on this list can be viewed but not edited.
	System administrators can modify the **Global Host Keys** list using the global ."The Known Hosts File" on page 451.

Multi-hop (Secure Shell Settings)

Use multi-hop connections when you need to establish secure connections through a series of Secure Shell servers. This is useful if your network configuration doesn't allow direct access to a remote server, but does allow access via intermediate servers.

The options are:

Multi-hop Servers	Display the servers in your multi-hop sequence. Reflection establishes a new SSH tunnel to the specified port on the remote server from the specified local port. Each connection on the list is sent through the tunnel established by the connection above it. You can change the list order using the arrow buttons.
Add (+)	Add a new server to the list using the **Configure Multi-hop Server** (page 479) dialog box.
Modify (✎)	Modify the selected server.
Delete (✕)	Delete the selected server.

◆ The settings you configure in this dialog box are saved to the Secure Shell configuration file (page 484). You can also configure Secure Shell settings by editing this file manually in any text editor.

◆ Within the configuration file, these settings are saved for the currently specified SSH configuration scheme (page 485).

Configure Multi-hop Server Dialog Box

Getting there

1 Open the **Reflection Secure Shell Settings** dialog box.

2 Click on the **Multi-hop** section.

3 Select **Add** (+).

Use this dialog box to add a server to your multi-hop list. The options are:

Starting local port	This is a port on your local Windows workstation. Multi-hop connections are forwarded from the specified port if it is available. If the port is in use, the port number is incremented until an available port is found.
Host name	Identify the host computer through which data will be sent.
Port	Specifies a port on the remote host to which data will be sent. The default is 22, which is the port used by most SSH servers.
User name	Specify a name here if this host requires a user name that's not the same as the one you specified for your original connection.
SSH config scheme	(Optional) Specify an SSH configuration scheme (page 485) to use for this connection. (Reflection uses the host name by default.)
Configure	Opens the Secure Shell settings dialog box, which you can use to configure non-default settings for this tunnel. Note: An alternate way to configure non-default settings is to specify an **SSH config scheme** for this connection.

PKI (Secure Shell Settings)

Use this section to configure PKI settings for Secure Shell sessions.

The options are:

Certificate host name must match host being contacted	Specifies whether host name matching is required when validating host certificates. When this setting is enabled (the default), the host name you configure for your session must exactly match a host name entered in either the **CommonName** or the **SubjectAltName** field of the certificate.

Use OCSP	Specifies whether Reflection checks for certificate revocation using OCSP (Online Certificate Status Protocol) responders when validating host certificates. OCSP responders may be specified in the AIA extension of the certificate itself. You can also specify OCSP responders using the **OCSP** tab in the Reflection Certificate Manager.
Use CRL	Specifies whether Reflection checks for certificate revocation using CRLs (Certificate Revocation Lists) when validating host certificates. CRLs may be specified in the CDP extension of the certificate itself. You can also specify CRL using the **LDAP** tab in the Reflection Certificate Manager.
	Note: The default value of this setting is based on your current system setting for CRL checking. To view and edit the system setting, launch Internet Explorer, and go to **Tools** > **Internet Options** > **Advanced.** Under **Security**, look for **Check for server certificate revocation**.
Reflection Certificate Manager	Opens the **Reflection Certificate Manager**, which you can use to manage certificates in the Reflection Certificate Manager store and to specify PKI settings.
View System Certificates	Opens the **Windows Certificate Manager**, which you can use to manage certificates in your system stores.

NOTE

- The settings you configure in this dialog box are saved to the Secure Shell configuration file (page 484). You can also configure Secure Shell settings by editing this file manually in any text editor.

- Within the configuration file, these settings are saved for the currently specified SSH configuration scheme (page 485).

Proxy (Secure Shell Settings)

Use the **Proxy** section to enable proxy use for Reflection Secure Shell sessions.

The options are:

Use Proxy Server	No proxy is configured. (This is the default.)
SOCKS	Select **SOCKS** to configure a Secure Shell connection through a SOCKS proxy.
HTTP	Select **HTTP** to configure a Secure Shell connection through an HTTP proxy.
Configure	Configure proxy server settings.

Tunneling (Secure Shell Settings)

Port forwarding allows you to forward TCP/IP traffic through an SSH tunnel. This allows you to use the Reflection Secure Shell Client to secure data that would otherwise be sent over an unsecured TCP/IP channel.

The options are:

Tunnel X11 connections	Specifies that all data sent from a remote X11 port is automatically forwarded through the secure tunnel to the correct local port.
Allow gateway ports	Enables gateway ports. Remote hosts are allowed to connect to local forwarded ports. By default, Reflection Secure Shell binds local port forwardings to the loopback address (this is equivalent to using "localhost"). This prevents other remote hosts from connecting to forwarded ports. **Allow gateway ports** can be used to specify that Reflection Secure Shell should bind local port forwardings to the local ethernet address (such as an IP address, a URL, or a DNS name), thus allowing remote hosts to connect to forwarded ports. Be careful about enabling this setting. Using it can reduce the security of your network and connection because it allows remote hosts to use the forwarded port on your system without authenticating.
Local forwarding	Displays local port forwarding you have configured. Click **Add** (+) to open the **Local Port Forwarding (page 481)** dialog box.
Remote forwarding	Displays remote port forwarding you have configured. Click **Add** (+) to open the **Remote Port Forwarding (page 482)** dialog box.

NOTE

- The settings you configure in this dialog box are saved to the Secure Shell configuration file (page 484). You can also configure Secure Shell settings by editing this file manually in any text editor.
- Within the configuration file, these settings are saved for the currently specified SSH configuration scheme (page 485).

Local Port Forwarding Dialog Box

Getting there

1 Open the **Reflection Secure Shell Settings** dialog box.

2 Click the **Tunneling** tab.

3 Under **Local Forwarding**, click **Add** (+).

Use this dialog box to configure local port forwarding. Outgoing data sent to the specified local port is forwarded through the secure tunnel to the specified remote host and port.

You must specify all of the following:

Forward local port	Specify any available port on your PC. Data sent to this port is forwarded through the SSH tunnel.
Destination Host Name	Identify the host computer to which data will be sent. (You can specify `localhost` to forward data to a different port on the same remote host to which you have already established a Secure Shell connection.)
Port	Specify the port on the remote host to which data will be sent. (This box is not available if you select **Tunnel Remote Desktop**, Reflection automatically configures the correct remote port.)
Forward Type	Available options are **TCP** and **FTP**. Use **TCP** unless you are forwarding communications between an **FTP** client and server.

You may also configure the following optional settings:

Tunnel Remote Desktop	Check this box to tunnel a Windows Remote Desktop session. When you select this option, other options become unavailable and Reflection automatically configures the correct settings to forward your session.
Use Reflection FTP	This button is visible only when **Forward Type** is set to FTP. When you click it, the values for **Application to Launch** are automatically filled in with the correct values to launch the Reflection FTP Client and tunnel your FTP communications.
Application to Launch Name	Enter a name to have Reflection automatically launch an application (for example a mail client, FTP client, or web browser) after the Secure Shell connection has been established. To use the secure tunnel, the application must be configured to connect to the port you set for **Forward local port**. With some applications you can do this using command line arguments, which you can specify in the **Arguments** text box.
Arguments	Specify optional command line arguments to use when the specified application is launched.

NOTE: Port forwarding settings are saved to the currently specified SSH configuration scheme (page 485).

Remote Port Forwarding Dialog Box

Getting there

1 Open the **Reflection Secure Shell Settings** dialog box.

2 Click the **Tunneling** tab.

3 Under **Remote Forwarding**, click **Add** (+).

Use this dialog box to configure remote port forwarding. Incoming data sent from the specified remote port is forwarded through the secure tunnel to the specified local computer and port.

You must specify all of the following:

Forward remote server port   Specifies a port on a host computer. Data sent from this port is forwarded to the PC through the SSH tunnel.

Name   Identifies the local computer to which data will be sent.

Port   Specifies the port on the local host to which data will be sent

---

NOTE: Port forwarding settings are saved to the currently specified SSH configuration scheme (page 485)

Getting to the Reflection Secure Shell Settings Dialog Box

The way you access the **Reflection Secure Shell Settings** dialog box depends on the session type you are in.

Terminal session

NOTE: Secure Shell connections are available for VT terminal sessions.

---

1 Open the Document Settings dialog box.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click .
TouchUx	Tap the Gear icon and then select **Document Settings**.

2 Click **Configure Connection Settings**.

3 Under **Network Connection Type**, select **Secure Shell**.

4 Under **Connection Options**, enter a host name.

5 Click **Security**.

FTP Client

1 In the **Connect to FTP Site** dialog box, click to select an FTP server.

2 Click **Security**.

3 Click the **Secure Shell** tab. **Use Reflection Secure Shell** must be selected.

4 (Optional) Specify an **SSH config scheme**. (If you leave **SSH config scheme** blank, Reflection saves any changes you make to an SSH configuration scheme (page 485) with the same name as the **Host name**.)

5 Click **Configure**.

Secure Shell Configuration File Reference Topics

In this Section

Secure Shell Client Configuration Files

The Secure Shell configuration file contains settings that are specific to the Secure Shell client connection. This user-specific file is created and updated automatically when you modify your settings using the "Reflection Secure Shell Settings Dialog Box" on page 469. Settings are saved automatically when you close this dialog box. The file name and location is:

```
My Documents \Micro Focus\Reflection\.ssh\config
```

Settings in this file are applied per host (or per SSH configuration scheme (page 485)) and affect both terminal session and FTP Client sessions. For example, when you configure non-default Secure Shell settings for a connection to Acme.com from a terminal session (and you don't specify an SSH configuration scheme), the Secure Shell settings are saved in the configuration file in a section identified with the following line:

```
Host Acme.com
```

If you also configure the FTP Client to connect to Acme.com (and you don't specify an SSH configuration scheme), the FTP Client uses the settings in the "Host Acme.com" section of the configuration file. (Settings are shared in the same way if you specify the same SSH configuration scheme in both applications.)

NOTE: When you close the Reflection Secure Shell Settings dialog box, values with default settings are not saved to the configuration file. If a default value has been manually added to the file, it is removed when you close the dialog box. This imposes design constraints if you use wildcard host stanzas in combination with stanzas that use specific host names. If you have manually configured a default value in a specific host stanza that is meant to override a value configured in a wildcard stanza, the default setting is removed when you open the Secure Shell settings dialog box to view settings for the host-specific SSH config scheme. You can successfully handle this situation by using the global configuration file, which is not updated when users open and close the Reflection Secure Shell Settings dialog box.

Global Configuration File

System administrators can also install a system-wide configuration file. The file name and location is:

```
%programdata%\Micro Focus\Reflection\ssh_config
```

Settings in this file affect client connections for all users of the computer.

Related Topics

SSH Configuration Schemes

Secure Shell configuration information is saved to your Secure Shell configuration file (page 485) using SSH configuration schemes. When you make a Secure Shell connection, Reflection uses the current SSH configuration scheme to determine how the connection should be made. Also, when you make any changes to your settings, Reflection saves those changes to the current SSH configuration scheme.

If you want to configure Secure Shell settings that are specific to a particular host, your SSH configuration scheme name should be the same as your host name.

NOTE: If you open the **Secure Shell Settings** dialog box without specifying a scheme, Reflection automatically creates a new SSH configuration scheme using the currently specified host name as soon as you change any of the Secure Shell settings.

If you want to use the same Secure Shell settings for connections to multiple hosts, enter a descriptive name for your SSH configuration scheme before you open the **Secure Shell Settings** dialog box, and then configure the settings you want to save to this scheme. Once you have created and configured the scheme, you can specify this scheme when you configure subsequent host sessions.

SSH configuration scheme names are case sensitive.

How SSH Configuration Schemes are Saved

Secure Shell configuration information is saved to your Secure Shell configuration file. SSH configuration scheme names are identified using the **Host** keyword. The configuration file is updated when you close the **Secure Shell Settings** dialog box. All non-default settings you configure are saved to the current scheme.

For an example, see "Sample Configuration File" on page 485.

Related Topics

Sample Configuration File

In this sample Secure Shell configuration file, there are two SSH configuration schemes — `MyHost.Demo.com` and `GeneralSSH`.

The settings under `MyHost.Demo.com` identify a set of Secure Shell settings using an actual host name. These settings will be used for all connections that specify MyHost.Demo.com as the SSH configuration scheme, and also for connections to that host when no SSH configuration scheme is specified.

Because `GeneralSSH` does not identify an actual host address, these settings will only be used if you specify this SSH configuration scheme when you configure your session.

With this config file, if you configure a connection to a new host (not MyHost.Demo.com) and you don't specify the `GeneralSSH` scheme, Reflection will connect using the default Secure Shell settings.

```
Host MyHost.Demo.Com
    Protocol 2
    KbdInteractiveAuthentication no
    ChallengeResponseAuthentication no
    PasswordAuthentication no
    RSAAuthentication no
    IdentityFile "C:\SSHusers\Joe\.ssh\mykey"
    LogLevel VERBOSE
#EndHost

Host GeneralSSH
    StrictHostKeyChecking yes
    ServerAlive yes
#EndHost
```

Related Topics

Configuration File Keyword Reference - Secure Shell Settings

Use this reference if you manually edit your Secure Shell configuration file (page 484). The configuration file is organized into sections, each identified by a **Host** keyword. Each section specifies Secure Shell settings to be used for all connections made using the specified host or SSH configuration scheme (page 485).

The configuration file consists of keywords followed by values. Configuration options may be separated by white space or by optional white space and exactly one equal sign (=). Keywords are case-insensitive and arguments are case-sensitive.

Any line starting with a number sign (#) is a comment. Any empty line is ignored.

NOTE: Items in this list configure features which affect the Secure Shell connection. Additional keywords are available for configuring terminal emulation for **ssh** command line sessions. Reference information about these keywords is available in "Configuration File Keyword Reference - Terminal Emulation Settings" on page 498.

AddAuthKeyToAgent

This setting affects how the client handles public key authentication when **ForwardAgent** is set to 'yes.' When public key authentication to the server is successful, and both **ForwardAgent** and **AddAuthKeyToAgent** are set to 'yes', the key or certificate that was used for authentication is automatically added to the Key Agent. This key is not saved in the Key Agent, but remains available as long as the Key Agent is running. When AddAuthKeyToAgent is set to 'no' (the default), keys and certificates are not automatically added to the Key Agent; it uses only those keys that have already been manually imported.

AgentEnumCertsAs

This setting allows the client to choose what it will use. When **both** is selected, the enumeration offers up both the certificate and the key as separate options. When **certs** are selected, the signing is requested using only the certificate. When **keys** is selected, a signing is requested using a key that was contained in a certificate, the agent now utilizes only the key. The order in which it is offered is set based on the initial connection. For example, if I connect using only a key, agent forwarding will enumerate the key, and then the certificate.

These values have been optimized to server types based on their currently supported algorithms and key types. Available optimization values= **sunssh**, **openvms**, **openssh**, **pkix** and **rsit**

AuthUseAllKeys

This setting affects how the client handles public key authentication. When this setting is 'no' (the default), the client attempts to authenticate using only the key (or keys) you have specified using the **IdentityFile** keyword. When this setting is 'yes' the client attempts to authenticate using all available public keys.

BatchMode

Specifies whether or not to disable all queries for user input, including password and passphrase prompts, which is useful for scripts and batch jobs. The allowed values are 'yes' and 'no'. The default is 'no'.

NOTE: This keyword does not disable queries for user input when keyboard interactive authentication is configured, but connections that use keyboard interactive will fail when **BatchMode** is enabled.

BindAddress

Specifies the interface to transmit from on computers with multiple interfaces or aliased addresses.

CheckHostIP

If this flag is set to 'yes', the Secure Shell Client checks the host IP address in the `known_hosts` file in addition to checking the host public key. The connection is allowed only if the host IP in the known hosts lists matches the IP address you are using for the connection. The default is 'no'. Note: This setting has no effect if **StrictHostKeyChecking** = no.

CheckHostPort

If this flag is set to 'yes', the Secure Shell Client checks the host port in the `known_hosts` file in addition to checking the host public key. The connection is allowed only if the host port in the known hosts lists matches the port you are using for the connection. The default is 'no'. Note: This setting has no effect if **StrictHostKeyChecking** = no.

Ciphers

Specifies the ciphers allowed for protocol version 2 in order of preference. Multiple ciphers must be comma-separated. The default is 'aes128-ctr,aes128-cbc,aes192-ctr,aes192-cbc,aes256-ctr,aes256-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour128,arcfour256,arcfour'.

ClearAllForwardings

Clears any local, remote, or dynamically forwarded ports that have already been processed from either a configuration file or the command line. Note: **scp** and **sftp** clear all forwarded ports automatically regardless of the value of this setting. The allowed values are 'yes' and 'no'. The default is 'no'.

Compression

Specifies whether compression is enabled. Compression is desirable on modem lines and other slow connections, but will slow down response rates on fast networks. Compression also adds extra randomness to the packet, making it harder for a malicious person to decrypt the packet. The allowed values are 'yes' and 'no'. The default is 'no'.

ConnectionAttempts

Specifies the number of tries (one per second) to make before exiting. The argument must be an integer. This may be useful in scripts if the connection sometimes fails. The default is 1.

ConnectionReuse

Specifies whether multiple sessions to the same host reuse the original Secure Shell connection, and, therefore don't require re-authentication. The argument must be 'yes' or 'no'. When set to 'yes' new connections reuse the existing tunnel when the host name, user name, and SSH configuration scheme (if used) all match. When set to 'no', Reflection establishes a new connection for each session, which means that each new connection repeats the authentication process and also applies any modified connection-specific settings (such as forwards and ciphers). The default is 'yes' for connections made using the Reflection window to make your connections. It is 'no' if you are using the command line utilities to make your connections. For details, see "Connection Reuse in Secure Shell Sessions" on page 443.

ConnectTimeout

Specifies the maximum time (in seconds) that the client waits when trying to complete the connection to the server. The timer starts when the connection is established (before logon) and runs during the negotiation of settings, host key exchange, and authentication. For all practical purposes, the timed period is basically the authentication activities. The default is 120.

DisableCRL

Specifies whether CRL (Certificate Revocation List) checking occurs when validating host certificates. Setting this to yes disables Certificate Revocation List checking. The default value of this setting is based on your current system setting for CRL checking. To view and edit the system setting, launch Internet Explorer, and go to **Tools** > **Internet Options** > **Advanced**. Under **Security**, look for "Check for server certificate revocation."

DynamicForward

Specifies that a TCP/IP port on the local machine be forwarded over the secure channel, and the application protocol is then used to determine where to connect to from the remote machine. The argument must be a port number. Currently the SOCKS4 protocol is supported, and Reflection Secure Shell will act as a SOCKS4 server. Multiple forwardings may be specified, and additional forwardings can be given on the command line. Only a user with administrative privileges can forward privileged ports.

EscapeChar

Sets the escape character (default: '~'). The escape character can also be set on the command line. The argument must be a single character, '^' followed by a letter, or 'none' to disable the escape character entirely (making the connection transparent for binary data).

FipsMode

When this setting is 'yes' connections must be made using security protocols and algorithms that meet United States government's Federal Information Processing Standard (FIPS) 140-2. Options that don't meet these standards are not available on the Encryption tab.

NOTE: This setting affects the SSH configuration scheme specified by the **Host** keyword, and has no effect on subsequent Secure Shell sessions unless they are configured to use the same SSH configuration scheme (or host name).

ForwardAgent

Setting this to 'yes' enables forwarding of the Key Agent connection. Agent forwarding should be enabled with caution. Users with the ability to bypass file permissions on the remote host (for the agent's Unix-domain socket) can access the local agent through the forwarded connection. Attackers cannot obtain key material from the agent, however they can perform operations on the keys that enable them to authenticate using the identities loaded into the agent. This may need to be enabled on the server also. The default is 'no'.

ForwardX11

Specifies whether X11 connections are automatically redirected over the secure channel and DISPLAY set. The argument must be 'yes' or 'no'. The default is 'no'. (Note: If you configure Secure Shell using Reflection X, see **ForwardX11ReflectionX**.)

ForwardX11ReflectionX

This setting is used only if you are configuring Secure Shell connections for Reflection X (starting with 14.1). It specifies whether X11 connections are automatically redirected over the secure channel and DISPLAY set. The argument must be "yes" or "no". The default is "yes".

GatewayPorts

Specifies whether remote hosts are allowed to connect to local forwarded ports. By default, Reflection Secure Shell binds local port forwardings to the loopback address. This prevents other remote hosts from connecting to forwarded ports. **GatewayPorts** can be used to specify that Reflection Secure Shell should bind local port forwardings to the wildcard address, thus allowing remote hosts to connect to forwarded ports. Be careful about enabling this setting. Using it can reduce the security of your network and connection because it can allow remote hosts to use the forwarded port on your system without authenticating. The argument must be 'yes' or 'no'. The default is 'no'.

GlobalKnownHostsFile

Specifies a file to use for the global host key database instead of the default file named ssh_known_hosts located in the Windows common application data folder.

NOTE: Enclose the filename in quotation marks if any part of the path or filename includes spaces.

GssapiAuthentication

Specifies whether GSSAPI authentication is used to authenticate to a KDC. This setting is applicable only if the protocol being used is protocol version 2.

GssapiDelegateCredentials

Specifies whether GSSAPI is used to forward your ticket granting ticket (krbtgt) to the host. This setting is applicable only if the protocol being used is protocol version 2.

GssapiUseSSPI

Specifies whether Microsoft's Security Support Provider Interface (SSPI) is used for GSSAPI authentication. This setting is applicable only if GSSAPI authentication is enabled (using **GssapiAuthentication** for protocol version 2). The argument to this keyword must be 'yes' or 'no'. When set to 'no' the Secure Shell Client uses GSSAPI authentication. When set to 'yes' the Secure Shell Client uses your Windows domain login credentials (SSPI) to authenticate to the Secure Shell server. SSPI is supported for protocol version 2 connections only, and the server must support the **GSSAPI-with-mic** authentication method. The default is 'yes'.

GssServicePrincipal

Specifies a non-default service principal name to use when the client sends a request for a service ticket to the Key Distribution Center (KDC). If you have selected SSPI for your GSSAPI provider, you can use this setting to specify a service principal in a realm that is different from the Windows domain. Use a fully qualified host name followed by @ then the realm name, for example `myhost.myrealm.com@MYREALM.COM`. (By default the hostname value is the name of the Secure Shell server to which you are connecting and the realm depends upon the value of **GssapiUseSSPI**. When **GssapiUseSSPI** is 'no' the realm name is specified in your default principal profile. When **GssapiUseSSPI** is 'yes', the realm is your Windows domain name.)

Host

Identifies the declarations that follow (up to the next **Host** key word) as belonging to the specified SSH configuration scheme (page 485). The characters '*' and '?' can be used as wildcards. A single '*' as a pattern can be used to provide global defaults for all hosts. A Reflection connection will use the first occurrence of any matching **Host** string (including wildcard characters). Any subsequent matches will be ignored.

NOTE: When you close the Reflection Secure Shell Settings dialog box, values with default settings are not saved to the configuration file. If a default value has been manually added to the file, it is removed when you close the dialog box. This imposes design constraints if you use wildcard host stanzas in combination with stanzas that use specific host names. If you have manually configured a default value in a specific host stanza that is meant to override a value configured in a wildcard stanza, the default setting is removed when you open the Secure Shell settings dialog box to view settings for the host-specific SSH configuration scheme. You can successfully handle this situation by using the global configuration file, which is not updated when users open and close the Reflection Secure Shell Settings dialog box.

HostKeyAlgorithms

Specifies, in order of preference, the host key algorithms that the client uses. The default for this option is: x509v3-ecdsa-sha2-nistp256,x509v3-ecdsa-sha2-nistp384,x509v3-rsa2048-sha256,x509v3-sign-rsa,x509v3-ssh-rsa,x509v3-sign-dss, ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,rsa-sha2-256, ssh-rsa-sha2-256@attachmate.com, ssh-rsa,ssh-dss.

This setting is useful when the server is configured for both certificate and standard host key authentication. The default value presents x509 algorithms before regular SSH key algorithms. SSH protocol allows only one attempt to authenticate the host. (This is different from user authentication in which multiple authentication methods and attempts are supported.) If the host presents a certificate, and the client is not configured for host authentication using certificates, the connection fails when x509 algorithms are preferred. In this situation you can configure the client to prefer SSH keys over certificates by changing the order of preference to ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,rsa-sha2-256,ssh-rsa-sha2-256@attachmate.com,ssh-rsa,ssh-dss,x509v3-ecdsa-sha2-nistp256,x509v3-ecdsa-sha2-nistp384,x509v3-rsa2048-sha256,x509v3-sign-rsa,x509v3-ssh-rsa,x509v3-sign-dss.

Available Values:ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,rsa-sha2-512,rsa-sha2-256,ssh-rsa-sha2-256@attachmate.com,ssh-rsa,ssh-dss,x509v3-ecdsa-sha2-nistp256,x509v3-ecdsa-sha2-nistp384,x509v3-ecdsa-sha2-nistp521,x509v3-rsa2048-sha256,x509v3-sign-rsa,x509v3-ssh-rsa,x509v3-sign-dss

HostKeyAlias

Specifies an alias to be used instead of the real host name for looking up or saving the host key in the host key database files. This option is useful for tunneling ssh connections or for multiple servers running on a single host.

IdentityFile

Specifies a private key to use for key authentication. Files are located in the user .ssh folder. (`\Users\`*username*`\Documents\Micro Focus\Reflection\.ssh\`). **IdentityFile** items are added when you select keys or certificates from the list in the **User Keys** tab of the **Secure Shell settings** dialog box. It is possible to have multiple identity files specified in configuration files; all these identities will be tried in sequence.

NOTE: Enclose the full path name in quotation marks if it includes spaces.

KbdInteractiveAuthentication

Specifies whether to use keyboard interactive authentication. The allowed values are 'yes' and 'no'. The default is 'yes'. This authentication method is recommended if you are using SecurID, PAM authentication, or any other external authentication method that requires prompts from the server and responses from the user. It may also work better than the **PasswordAuthentication** method for password authentication on hosts where password expiration or first login password changing is enabled. It may also be required for password authentication when expired passwords need to be reset in order to successfully authenticate. This applies to SSH protocol 2 only.

KeepAlive

Specifies whether the system should send TCP keepalive messages to the other side. If they are sent, death of the connection or crash of one of the machines will be detected. The default is 'yes' (to send keepalives), so that the client will detect that the network goes down or the remote host dies. This is important in scripts and helpful to users. However, this means that connections will die if the route is down temporarily, which some users find annoying. To disable keepalives, set the value to 'no'. This keyword enables the Windows TCP keep alive setting, which sends keep alive messages every two hours by default. TCP/IP keep alive is configurable using two optional pentameters that typically do not exist in the Windows registry: KeepAliveTime and KeepAliveInterval. These are configured in the `HKEY_LOCAL_MACHINE` registry subtree, in the following location:

```
SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
```

For information about setting these parameters, refer to Microsoft Knowledge Base Article 120642.

KexAlgorithms

Specifies which key exchange algorithms the client supports, and the order of preference. The supported values are 'ecdh-sha2-nistp256', 'ecdh-sha2-nistp384', 'ecdh-sha2-nistp521', 'diffie-hellman-group1-sha1', 'diffie-hellman-group-exchange-sha1' and 'diffie-hellman-group14-sha1'. The default is 'ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group1-sha1,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1'.

LocalForward

Specifies that a TCP/IP port on the local machine be forwarded over the secure channel to the specified host and port on the remote machine. Multiple forwardings can be specified. Only users with administrator privileges can forward privileged ports. You can also configure optional arguments for forwarding FTP, configuring remote desktop, and automatically launching an executable file (*.exe) after the connection is made. The syntax for this keyword is:

```
LocalForward localport host: hostport [FTP=0|1] [RDP=0|1] [" ExecutableFile "
[args]]
```

The options are:

localport	A local port number.
host: *hostport*	A remote host and a port on that host. (You can specify `localhost` to forward data to a different port on the same remote host to which you have already established a Secure Shell connection.) IPv6 addresses can be specified with an alternative syntax: `host/port`.
FTP	Set to `1` if you are tunneling FTP file transfer.
RDP	Set to `1` if you are tunneling a Remote Desktop session.
" *ExecutableFile* "	Specify an executable file (including complete path information, if required) to have Reflection launch an application immediately after the Secure Shell connection is established. To forward data through the secure tunnel, this application should be configured to make a connection to *localhost* (or the loopback IP address, `127.0.0.1`) using the specified *localport*.

Logfile

Specifies a log file to use for debugging. All session input and output is written to this file. Use this keyword with the **-o** command-line utility option as shown here:

```
-o Logfile=\ path\ logfile_name
```

NOTE: Enclose the path filename in quotation marks if any part of the path or filename includes spaces.

LogLevel

Specifies the verbosity level that is used when logging messages from the Secure Shell Client. The possible values are: QUIET, FATAL, ERROR, INFO, VERBOSE, DEBUG, DEBUG1, DEBUG2 and DEBUG3. The default is INFO. DEBUG and DEBUG1 are equivalent. DEBUG2 and DEBUG3 each specify higher levels of verbose output.

Macs

Specifies the MAC (message authentication code) algorithms in order of preference. The MAC algorithm is used in protocol version 2 for data integrity protection. Multiple algorithms must be comma-separated. The default is: "hmac-sha256, hmac-sha2-256, hmac-sha1, hmac-md5, hmac-ripemd160, hmac-sha1-96, hmac-md5-96, hmac-sha512, hmac-sha2-512."

MatchHostName

Specifies whether host name matching is required when validating host certificates. When this setting is 'yes' (the default), the host name you configure for your connection must exactly match a host name entered in either the CommonName or the SubjectAltName fields of the certificate.

Multihop

Configures multi-hop connections, which can be used to establish secure connections through a series of SSH servers. This is useful if your network configuration doesn't allow direct access to a remote server, but does allow access via intermediate servers.

The syntax for this keyword is:

`Multihop` *localport* `host:` *hostport* [**"** *SSH config scheme* **"**]

Add a new **Multihop** line for each server in the series. Each connection on the list is sent through the tunnel established by the connection above it.

In the example below, SSH connections configured to ServerC will connect first to ServerA, then to ServerB, and finally to the ServerC.

```
Host ServerC
Multihop 2022 ServerA:22
Multihop 3022 ServerB:22
```
You can optionally specify an to configure Secure Shell settings for any host in the chain. For example:

```
Multihop 4022 joe@ServerA:22 "Multihop SchemeA"
```

Nodelay

This setting addresses a change made by Microsoft that enables the Nagle algorithm on Windows tcp sockets by default, and can adversely affect performance in Secure Shell connections. Setting **Nodelay** to yes (the default) disables this algorithm and improves performance on most systems.

NoShell

When **NoShell** is set to "Yes", the client creates a tunnel without opening a terminal session. This option can be used in combination with ConnectionReuse to create a tunnel that can be reused by other ssh connections. Note: This option affects connections made with the command line utility; it is not intended for use with the user interface.

NumberOfPasswordPrompts

Specifies the number of password prompts before giving up. The argument to this keyword must be an integer. The default is 3.

PasswordAuthentication

Specifies whether to use password authentication. The allowed values are 'yes' and 'no'. The default is 'yes'.

Port

Specifies the port number to connect on the remote host. The default is 22.

PreferredAuthentications

Specifies the order in which the client should try protocol 2 authentication methods. This corresponds to the order (top to bottom) in which the methods are displayed in the **User Authentication** list on the **General** tab of the **Reflection Secure Shell Settings** dialog box. This setting enables the client to prefer one method (such as keyboard-interactive) over another method (such as password). By default, Reflection attempts authentication in the following order: 'publickey,keyboard-interactive,password'. If GSSAPI authentication is enabled, the default changes to: 'gssapi-with-mic,external-keyex,gssapi,publickey,keyboard-interactive,password'.

NOTE

- If you include **PreferredAuthentications** in your config file, the list you specify must include every authentication method you want to try. If **PreferredAuthentications** is present, but does not specify a particular authentication method, Reflection will not use that authentication method, even if the keyword for enabling that authentication method is correctly configured.

- Including an authentication method in the **PreferredAuthentications** list does not enable authentication using that method. To enable an authentication method that is not used by default, the keyword for that authentication method must also be correctly configured (for example, to enable GSSAPI authentication, you must set **GssapiAuthentication** to yes.)

PreserveTimestamps

Specifies whether file attributes and timestamps are modified when files are transferred to and from the server. When this keyword is "no" (the default), timestamps and attributes are modified. When it is "yes", the files retain their original timestamps and attributes.

Protocol

The Secure Shell Client supports protocol 2, which is identified as the value '2'.

Proxy

Specifies a proxy type to use for Secure Shell connections. Supported values are "SOCKS" and "HTTP".

NOTE: Proxy use is enabled for each **Host** section in the configuration file using this setting. The proxy server address is stored in the Windows registry on a per-user basis.

PubkeyAlgorithms

Specifies in order of preference the key algorithms the client will propose to the server. If the server is only configured for one algorithm you can set this keyword to only propose that option.

Available values:ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,rsa-sha2-512,rsa-sha2-256,ssh-rsa-sha2-256@attachmate.com,ssh-rsa,ssh-dss,x509v3-ecdsa-sha2-nistp256,x509v3-ecdsa-sha2-nistp384,x509v3-ecdsa-sha2-nistp521x509v3-rsa2048-sha256,x509v3-sign-rsa,x509v3-ssh-rsa,x509v3-sign-dss

PubkeyAuthentication

Specifies whether to try public key authentication. This option applies to protocol version 2. The allowed values are 'yes' and 'no'. The default is 'yes'.

RemoteCommand

Specifies one or more commands to run on the remote server. Use a semicolon (;) to separate multiple commands when connecting to a UNIX server. Use an ampersand (&) to separate commands when connecting to a Windows server. After a connection is established the server executes (or attempts to execute) the specified command(s), and then the session terminates. The server must be configured to allow commands received from the client to run.

The commands must be specified using the correct syntax for your server. For example, the following are equivalent:

On UNIX: `ls ; ls -l`

On Windows: `dir/w & dir`

RemoteForward

Specifies that a TCP/IP port on the remote machine be forwarded over the secure channel to the specified host and port from the local machine. The first argument must be a port number, and the second must be *host* `:` *port*. IPv6 addresses can be specified with an alternative syntax: *host* / *port*. Multiple forwardings may be specified. Only the users with administrator privileges can forward privileged ports.

SendEnv

Specifies an environment variable to set on the server before executing a shell or a command. The value should be of form: `VAR val`. The server must support the specified variable, and must be configured to accept these environment variables.

ServerAlive

Specifies whether to send server alive messages to the SSH server at the interval specified by **ServerAliveInterval**. The Secure Shell **ServerAlive** setting sends an SSH protocol message to the server at the specified interval to ensure that the server is still functioning. If this is setting is not enabled, the SSH connection will not terminate if the server dies or the network connection is lost. This setting can also be used to keep connections that only forward TCP sessions from being timed out by the server, as the server may timeout these connections because it detects no SSH traffic. The allowed values are 'yes' and 'no'. The default is 'no'.

NOTE: The Secure Shell **ServerAlive** setting is not related to the TCP keep alive setting (KeepAlive) that can be set in the Windows registry to keep all TCP/IP connections from being timed out by a firewall. To change the TCP/IP keep alive behavior, you need to edit the Windows registry.

ServerAliveInterval

Specifies the interval (in seconds) to use when **ServerAlive** = 'yes'. Use an integer value of one or greater. The default is 30.

ServerKeyFormat

Specifies the key format to use when uploading keys to a Host using the Upload feature on the User Keys tab. The utility automatically determines which the key format to use. Modify this setting if that format is incorrect for your server. The allowed values are 'OpenSSH' and 'SECSH'.

ServerStyle

Specifies the host public key configuration settings to use when uploading keys to a Host using the Upload feature on the User Keys tab. The utility automatically determines which host style to use. Modify this setting if that format is incorrect for your server. The allowed values are 'UNIX' and 'VMS'.

SftpBufferLen

Specifies the number of bytes requested in each packet during SFTP transfers. The default is 32768. Adjusting this value can improve transfer speed. The optimum value depends on your network and server setup. Changing this value may also affect how quickly you can cancel a transfer.

SftpMaxRequests

Specifies the maximum number of outstanding data requests that the client will allow during SFTP transfers. The default is 10. Adjusting this value can improve transfer speed. The optimum value depends on your network and server setup. Changing this value may also affect how quickly you can cancel a transfer.

SftpVersion

Specifies which version the client uses for SFTP connections. Valid values are 3 and 4. When this setting is 4 (the default), the connection uses SFTP version 4 if the server supports it, and drops to version 3 if the server doesn't support version 4. If this setting is 3, the client always uses SFTP version 3.

StrictHostKeyChecking

The argument must be 'yes', 'no' or 'ask'. The default is 'ask'. If this option is set to 'yes', the Secure Shell Client never automatically adds host keys to the known_hosts file (located in the user .ssh folder), and refuses to connect to hosts whose host key has changed. This option forces the user to manually add all new hosts. If this flag is set to 'no', Reflection connects to the host without displaying a confirmation dialog box, and does not add the host key to the list of trusted keys. If this flag is set to 'ask', new host keys are added to the user known host files only after the user has confirmed that is what they want. The host keys of known hosts are verified automatically in all cases.

NOTE: This setting has no effect when the host has been configured to authenticate using x509 certificates. If a host presents a certificate for host authentication and you do not have the required CA certificate configured as a trust anchor, the connection will fail.

TryEmptyPassword

If this flag is set to 'yes' , the client starts the password authentication by trying to enter an empty password. Note that this will count as a login attempt on most systems.

User

Specifies the user to log in as. This can be useful when a different user name is used on different machines.

UseOCSP

Specifies whether the client uses OCSP (Online Certificate Status Protocol) to validate host certificates. The allowed values are 'yes' and 'no'. The default is 'no'.

UserKeyCertLast

Specifies how the client handles the signature for certificates during public key authentication. When this setting is '**yes**' (the default), the client sends the certificate using a standard ssh key signature first. If that fails, the client tries again using a certificate signature. In some cases this second attempt may not occur and authentication fails. When this setting is '**no**', the client tries the certificate signature first followed by the ssh key signature.

UserKnownHostsFile

Specifies a file to use for the user host key database instead of the `known_hosts` file (located in the user .ssh folder). Use quotation marks if the file or path includes spaces.

x509dsasigtype

Specifies the hash algorithm the client uses in the process of proving possession of DSA private keys. Possible values are 'sha1raw' (the default) and 'sha1asn1'.

x509rsasigtype

Specifies the hash algorithm the client uses in the process of proving possession of RSA private keys. Possible values are 'md5', 'sha1', and 'sha256' and 'all' (the default).

X11Display

Determines the port on the PC's local loopback interface to which X11 protocol communications are forwarded when X11 forwarding in enabled.

NOTE: If you are using Reflection X (version 12.x, 13.x, or 14.x), you don't need to configure this keyword. The Reflection X server and Secure Shell client automatically synchronize to use the correct port based on your X server display setting (**Settings** > **Display** > **X display number**); in this case the **X11Display** keyword is ignored. If you use a different PC X server, use this keyword to specify the correct listening port as defined for your PC X server.

The default value is 0. This configures forwarding to port 6000, which is the default listening port defined by X11 protocol convention. The display value you specify is added to 6000 to determine the actual listening port. For example, setting **X11Display** to 20 indicates to the Secure Shell client that the PC-X server is listening on port 6020.

Related Topics

- "Configuration File Keyword Reference - Terminal Emulation Settings" on page 498

Configuration File Keyword Reference - Terminal Emulation Settings

Items in this list configure terminal emulation settings for **ssh** (page 505) and **ssh2** command line sessions. These settings can be implemented by adding them manually to the Secure Shell configuration file (page 484), or by using the -o switch on the command line.

> **NOTE:** These settings affect command line terminal sessions only; they have no affect on terminal sessions running in the Reflection user interface.

The configuration file is organized into sections, each identified by a **Host** keyword. Each section specifies settings to be used for all connections made using the specified host or SSH configuration scheme (page 485).

The configuration file consists of keywords followed by values. Configuration options may be separated by white space or by optional white space and exactly one equal sign (=). Keywords are case-insensitive and arguments are case-sensitive.

Any line starting with a number sign (#) is a comment. Any empty line is ignored.

Quotation marks are required around string arguments that include spaces. Terminal emulation keywords and arguments are not case-sensitive.

> **NOTE:** Keywords for configuring Secure Shell connections are available in a separate list. See "Configuration File Keyword Reference - Secure Shell Settings" on page 486.

AnswerBackMessage

When **AutoAnswerback** is set to 'yes', **AnswerBackMessage** specifies the string that is sent to the host in response to an answerback request (the ENQ character-ASCII 5).

Possible String Values: A string value of up to 30 characters.
Default: "" (null string)
Sample syntax:

```
AutoAnswerback yes
AnswerbackMessage "My answer back string"
```

AutoAnswerback

When **AutoAnswerback** is set to yes, the message string specified using the **AnswerBackMessage** keyword is automatically sent to the host after a connection is made.

Possible Values: yes or no
Default: no
Sample syntax:

```
AutoAnswerback yes
AnswerbackMessage "My answer back string"
```

AutoWrap

Determines what happens when the cursor reaches the right margin. When set to yes, characters will wrap to the next line automatically when the cursor reaches the right margin of the terminal window. When set to no, the cursor is not automatically advanced when it reaches the right margin-as you type additional characters, each character overwrites the previous character until you move the cursor.

Possible Values: yes or no
Default: no
Sample syntax:

```
AutoWrap yes
```

BackspaceKeyIsDel

Specifies the behavior of the backspace key. When set to no, the backspace key transmits a backspace (ASCII 8) character. When set to yes, the backspace key transmits the delete (ASCII 127) character.

Possible Values: yes or no
Default: no
Sample syntax:

```
BackspaceKeyIsDel yes
```

CursorKeyMode

Specifies how the client handles keys on the cursor keypad. When set to no, the cursor keypad is set to normal mode-the cursor keypad keys transmit cursor escape sequences. When set to yes, the cursor keypad is set to application mode-cursor keypad keys will transmit application escape sequences.

Possible Values: yes or no
Default: no
Sample syntax:

```
CursorKeyMode yes
```

CursorStyle

Specifies the cursor style.

Possible String Values: Block, Blockblink, Line, Lineblink
Default: Lineblink
Sample syntax:

```
CursorStyle Block
```

CursorVisible

Specifies whether the cursor is visible. When set to no, the cursor is not visible in the terminal window.

Possible Values: yes or no
Default: yes
Sample syntax:

```
CursorVisible no
```

DisplayCols

Sets the number of columns in the terminal window.

Possible Values: The minimum is 80. The maximum usable value depends on your monitor size and display settings.
Default: Determined by the current command window size.
Sample syntax:

```
DisplayCols 120
```

DisplayRows

Sets the number of rows in the terminal window.

Possible Values: The minimum is 24. The maximum usable value depends on your monitor size and display settings.
Default: Determined by the current command window size.

Sample syntax:

```
DisplayRows 30
```

HostCharacterSet

Specifies a non-default host character set.

Possible String Values:

PC437_English	Windows1256
PC737_Greek	Windows1257
PC775_Baltic	Windows1258
PC850_Multilingual	Korean_Johab
PC852_Slavic	ISOLatin_1
PC855_Cyrillic	ISOLatin_2
PC857_Turkish	ISOLatin_3
PC858_Multilingual_Euro	ISO_Baltic
PC860_Portuguese	ISO_Cyrillic
PC861_Icelandic	ISO_Arabic
PC862_Hebrew	ISO_Greek
PC863_CanadianFrench	ISO_Hebrew
PC864_Arabic	ISOLatin_5
PC865_Nordic	ISOLatin_9
PC866_Cyrillic	ISO2022_JIS
PC869_ModernGreek	ISO2022_JIS-Allow
PC932_Shift_JIS	ISO2022_JIS-X0201_1989
PC936_SimplifiedChinese	ISO2022_Korean
PC949_Korean	ISO2022_SimplifiedChinese
PC950_TraditionalChinese	ISO2022_TraditionalChinese
DECMultinational	EUC_Japanese
UCS2	EUC_SimplifiedChinese
Windows1250	EUC_Korean
Windows1251	EUC_TraditionalChinese
Windows1252	GB2312_SimplifiedChinese
Windows1253	GB18030_SimplifiedChinese
Windows1254	UTF7
Windows1255	UTF8

Default: PC437_English

Sample syntax:

```
HostCharacterSet EUC_Japanese
```

InsertMode

Specifies whether typing is in insert or replace mode. When set to no, typing replaces existing characters at the cursor location. When set to yes, new characters are inserted at the cursor location, and existing characters are moved to the right.

Possible Values: yes or no
Default: no

Sample syntax:

```
InsertMode yes
```

InverseVideo

Specifies whether the terminal window uses inverse video. When set to yes, foreground and background colors for all screen attributes are reversed.

Possible Values: yes or no
Default: no
Sample syntax:

```
InverseVideo yes
```

KeyBoardActionMode

Specifies whether the keyboard is available. When set to yes, the keyboard is locked and cannot be used.

Possible Values: yes or no
Default: no
Sample syntax:

```
KeyBoardActionMode yes
```

MarginBell

Determines whether a margin bell sounds. When set to yes, the bell sounds when the cursor is eight characters from the right margin. Set this setting to no to prevent sounding the margin bell.

Possible Values: yes or no
Default: yes
Sample syntax:

```
MarginBell no
```

NewLine

Specifies whether the client is in linefeed or newline mode. When set to no (linefeed mode), pressing the Enter key sends only a carriage return. Received linefeeds, formfeeds, and vertical tabs move the cursor down one line in the current column. When set to yes (newline mode), pressing the Enter key sends both a carriage return and a linefeed. Received formfeeds, and vertical tabs move the cursor to the first column of the next line.

Possible Values: yes or no
Default: no
Sample syntax:

```
NewLine yes
```

NRCSet

Use one of the supported string values to specify a different National Replacement Character set. You must also set the **UseNRC** keyword to yes to enable this.

Possible String Values:

British	Norwegian
Finnish	Portuguese
French	EuropeanSpanish
CanadianFrench	Swedish
German	SwissGerman
Italian	

Default: ASCII
Sample syntax:

```
UseNRC yes
NRCSet British
```

NumericKeyPadMode

Specifies how the client handles the keys on the numeric key pad. When set to yes, the keypad is set to numeric mode — the keypad keys transmit numeric values when pressed. When set to no, the keypad is set to application mode — the keypad keys transmit application escape sequences such as home, up, and right.

Possible Values: yes or no
Default: no
Sample syntax:

```
NumericKeyPadMode no
```

OriginMode

Specifies the cursor's home position. When set to no, the cursor's home position is at the upper-left hand corner of the terminal window. When set to yes the cursor's home position is relative to the terminal windows margin settings.

Possible Values: yes or no
Default: no
Sample syntax:

```
OriginMode yes
```

SevenBitControls

Specifies how 8-bit C1 control codes are transmitted. When set to yes, 7-bit equivalents are transmitted for the 8-bit C1 control codes. When set to no, 8-bit C1 control codes are transmitted.

NOTE: The default value for **HostCharacterSet** for the **ssh** command line client is PC437_English. If you want to send C1 controls, you need to set **HostCharacterSet** to DECMultinational or one of the ISOLatin character sets.

Possible Values: yes or no
Default: yes
Sample syntax:

```
SevenBitControls no
```

TerminalModel

Specifies which terminal type the client emulates.

Possible String Values: vt52, vt102, vt220
Default: vt220
Sample syntax:

```
TerminalModel vt102
```

UseNRC

When this is set to yes, you can specify a National Replacement Character set using the **NRCSet** keyword.

Possible Values: yes or no
Default: no
Sample syntax:

```
UseNRC yes
NRCSet British
```

UseANSIColor

When set to yes, ANSI color escape sequences are supported.

Possible Values: yes or no
Default: yes
Sample syntax:

```
UseANSIColor no
```

WarningBell

Specifies whether a warning bell sounds. When set to yes, the bell sounds when a bell character (ASCII 7) is received from the host or entered from the keyboard. Set this setting to no to prevent sounding the warning bell.

Possible Values: yes or no
Default: yes
Sample syntax:

```
WarningBell no
```

Related Topics

◆ "Configuration File Keyword Reference - Secure Shell Settings" on page 486

Deploy Secure Shell Settings with a Companion Installer

System administrators can use the Installation Customization Tool to deploy Secure Shell settings to end users. You can specify both user-specific and global locations for installing files.

NOTE: For names and locations of configuration files used by Secure Shell sessions, see the lists that follow the procedure

---

To create a companion package to install Secure Shell settings

1 Configure the Secure Shell settings you want to deploy.

2 Create an administrative installation of Reflection (or use an existing one).

3 From your administrative installation point, open the Installation Customization Tool from a shortcut or by typing the following command line:

   <path_to_setup> `\setup.exe /admin`

4 From the **Select Customization** dialog box, select **Create a new Companion installer** (or open an existing MSI), and then click **OK**.

5 From the navigation pane, select **Specify install locations**.

6 Under **Installation type**, specify either **Installs to all users of a machine** or **Installs only for the user who installs it**.

7 From the navigation pane, select **Add files**.

8 Under **Add files to**, specify a destination location. Refer to the lists that follow this procedure.

9 Click **Add**, browse to locate the file you want to add to the installation, then click **Open**.

10 Click **File** > **Save As** and enter a name for your installer file (for example `SecureShellSettings.msi`).

User-specific files and locations

File Name	Add File To
`config`	[`PersonalFolder`]\Micro Focus\Reflection\.ssh **NOTE:** For information about this file, see "Secure Shell Client Configuration Files" on page 484.
`known_hosts`	[`PersonalFolder`]\Micro Focus\Reflection\.ssh **NOTE:** For information about this file, see "The Known Hosts File" on page 451.
`pki_config`	[`PersonalFolder`]\Micro Focus\Reflection\.pki **NOTE:** This file configures Reflection Certificate Manager settings.
`trust_store.p12`	[`PersonalFolder`]\Micro Focus\Reflection\.pki **NOTE:** This file configures Reflection Trusted Certificate Authorities

Global files and locations

File Name	Add File To
`ssh_config`	[`CommonAppDataFolder`]\Micro Focus\Reflection\ **NOTE:** This is the global Secure Shell client configuration file.
`ssh_known_hosts`	[`CommonAppDataFolder`]\Micro Focus\Reflection\ **NOTE:** This is the global known hosts file.
`pki_config`	[`CommonAppDataFolder`]\Micro Focus\Reflection\.pki
`trust_store.p12`	[`CommonAppDataFolder`]\Micro Focus\Reflection\.pki

Command Line Utilities

Reflection Secure Shell support includes DOS command-line utilities. The executable files that support these utilities are installed to your PC in the same location as your Reflection program files.

In this Section

ssh Command Line Utility

Syntax: ssh [options] [user@]hostname [host command]

You can use the **ssh** command line utility to make Secure Shell connections from the Windows command line.

NOTE

- Some Micro Focus products provide an **ssh2** utility. Both **ssh** and **ssh2** can be used to establish Secure Shell connections, but some of the options supported by these two utilities are different. The **ssh** client is recommended. The **ssh2** options are compatible with the Reflection for Secure IT UNIX client and the F-Secure client. Use command line help (`ssh2 -h`) for a description of the options available with **ssh2**.

- You can reuse an existing Secure Shell connection. However, to do so you must explicitly enable this on each command line, or set the SSHConnectionReUse environment variable to Yes. For details, see Connection Reuse in Secure Shell Sessions (page 443).

Options

-A

Enables authentication agent forwarding. This can also be specified on a per-host basis in a configuration file (page 486). Agent forwarding should be enabled with caution. Users with the ability to bypass file permissions on the remote host can access the local agent through the forwarded connection. Attackers cannot obtain key material from the agent, however they can perform operations on the keys that enable them to authenticate using the identities loaded into the agent.

-a

Disables authentication agent forwarding. (This is the default.)

-b *bind_address*

Specify the interface to transmit from on machines with multiple interfaces or aliased addresses.

-c *cipher_spec*

A comma-separated list of ciphers specified in order of preference. The default is "aes128-ctr,aes128-cbc,aes192-ctr,aes192-cbc,aes256-ctr,aes256-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour128,arcfour256,arcfour".

-C

Enables compression of all transmitted data. Compression is desirable on modem lines and other slow connections, but will only slow down response rate on fast networks.

-e *escape_character*

Sets the escape character for the terminal session. The default character is a tilde (~). Setting the escape character to `none' means that no escape character is available and the tilde acts like any other character. The following escape sequences are available. (Replace the tilde with your designated escape_character.)

`~.` Terminate the connection.
`~R` Request rekey (SSH protocol 2 only).
`~#` List forwarded connections.
`~?` Display available escape sequences.
`~~` Type the escape character twice to send it to the host.

-E *provider*

Uses the specified provider as the external key provider.

-f

Places the client in the background just before command execution.

-F *config_file*

Specifies an alternate configuration file to use for this connection. If a configuration file is given on the command line, other configuration files (page 484) are ignored.

-g

Enables gateway ports. Remote hosts are allowed to connect to local forwarded ports.

-h

Displays a summary of command line options.

-H *scheme*

Specifies which SSH configuration scheme (page 485) to use for this connection.

-i *key_file*

Specifies a private key to use for key authentication. Key files can also be specified on a per-host basis in the configuration file (page 486). It is possible to have multiple `- i` options (and multiple keys specified in a configuration file). Use quotation marks if the file or path includes spaces.

-k *directory*

Specifies an alternate location for the config, host key, and user key files. Note: When -k is used, host keys are read and written from the specified location only if a known-hosts file already exists in that location. If no known-hosts file is found, host keys are read and written to the known-hosts file in the default location.

-l *login_name*

Specifies a name to use for login on the remote computer. This can also be specified in the configuration file (page 486).

-L *localport:remotehost:hostport*

Redirects data from the specified local port, through the secure tunnel to the specified destination host and port. Local Port Forwarding. Port forwardings can also be specified in the configuration file. You cannot forward privileged ports (port numbers below 1024) unless you are logged in as an administrator. IPv6 addresses can be specified with an alternative syntax: `port/host/hostport`.

-m *mac_spec*

Specifies one or more comma-separated MAC (message authentication code) algorithms to use for this connection. Specify algorithms in order of preference. The default is "hmac-sha1,hmac-sha256,hmac-sha512,hmac-md5,hmac-ripemd160,hmac-sha1-96,hmac-md5-96". If the connection is set to run in FIPS mode, the default is "hmac-sha1,hmac-sha256,hmac-sha512".

-N

Do not execute a remote command. This is useful for configuring just port forwarding. (protocol version 2 only).

-o *option*

Sets any option that is supported in the configuration file (page 486). For example:

`ssh "-o FIPSMode=yes" myuser@myhost`

-p *port*

Specifies the port to connect to on the server. The default is 22, which is the standard port for Secure Shell connections. This can be specified on a per-host basis in the configuration file (page 486).

-q

Enables quiet mode, which causes all warning and diagnostic messages, including banners, to be suppressed.

-R *localport:remotehost:hostport*

Redirects data from the specified remote port (on the computer running the Secure Shell server), through the secure tunnel to the specified destination host and port. Remote Port Forwarding. Port forwardings can also be specified in the configuration file. You cannot forward privileged ports (port numbers below 1024) unless you are logged in as an administrator. IPv6 addresses can be specified with an alternative syntax: `port/host/hostport`.

-S

Do not execute a shell.

-t

Forces a tty allocation even if a command is specified.

-T

Disable pseudo-tty allocation.

-v

Sets the debug level to verbose mode, which is equivalent to setting the debug level to 2.

-V

Displays product name and version information and exits. If other options are specified on the command line, they are ignored.

-x

Disables X11 connection forwarding.

-X

Enables X11 connection forwarding and treats X11 clients as untrusted. Untrusted remote X11 clients are prevented from tampering with data belonging to trusted X11 clients.

X11 forwarding should be enabled with caution. Users with the ability to bypass file permissions on the remote host (for the user's X authorization database) can access the local X11 display through the forwarded connection. An attacker may then be able to perform activities such as keystroke monitoring.

-Y

Enables X11 connection forwarding and treats X11 clients as trusted.

X11 forwarding should be enabled with caution. Users with the ability to bypass file permissions on the remote host (for the user's X authorization database) can access the local X11 display through the forwarded connection. An attacker may then be able to perform activities such as keystroke monitoring.

-1

Forces **ssh** to try protocol version 1 only. Protocol version 1 is deprecated and not recommended.

-2

Forces **ssh** to try protocol version 2 only.

-4

Forces connections using IPv4 addresses only.

-6

Forces connections using IPV6 addresses only

sftp Command Line Utility

Syntax:

```
sftp [
options
] [
user
@]
host
[#
port]
:
source_file
 [
user
@]
host
[#
port
][:
destination_file
]
```

NOTE: You can reuse an existing Secure Shell connection. However, to do so you must explicitly enable this on each command line, or set the SSHConnectionReUse environment variable to Yes. For details, see "Connection Reuse in Secure Shell Sessions" on page 443.

Command Line Options

-a

Transfer files in ASCII mode.

-b *buffersize*

Sets the maximum buffer size for one request. Valid values are 1024 - 32768.

-B *batchfile*

After a successful login, executes each command in the specified batch file and then terminates the connection. For example, the following command connects to `myhost` using `myname` and executes the commands in `myfile`. After all commands in the file are executed, the connection is terminated.

```
sftp -B c:\mypath\myfile myhost.com myname
```

The batch file can use any of the interactive commands documented below.

NOTE: Semicolons are not supported for comments in scripts supplied to the **sftp** command line using the **-B** option. Use the number sign (#) to mark comments in these batch files.

-c *cipher*

A comma-separated list of ciphers specified in order of preference. The default is "aes128-ctr,aes128-cbc,aes192-ctr,aes192-cbc,aes256-ctr,aes256-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour128,arcfour256,arcfour".

Protocol version 1 (which is deprecated and not recommended) allows specification of a single cipher. The supported values are "3des", "blowfish", and "des".

-C

Enables compression of all transmitted data. Compression is desirable on modem lines and other slow connections, but will only slow down response rate on fast networks.

-d

Force target to be a directory.

-F *config_file*

Specifies an alternate configuration file to use for this connection. If a configuration file is given on the command line, other configuration files (page 484) are ignored.

-h

Displays a summary of command line options.

-H *scheme*

Specifies which SSH configuration scheme (page 485) to use for this connection.

-i *key_file*

Specifies a private key to use for key authentication. Key files can also be specified on a per-host basis in the configuration file (page 484). It is possible to have multiple - i options (and multiple keys specified in a configuration file). Use quotation marks if the file or path includes spaces.

-k *directory*

Specifies an alternate location for the config, host key, and user key files. Note: When -k is used, host keys are read and written from the specified location only if a known-hosts file already exists in that location. If no known-hosts file is found, host keys are read and written to the known-hosts file in the default location.

-m *mac_spec*

Specifies one or more comma-separated MAC (message authentication code) algorithms to use for this connection. Specify algorithms in order of preference. The default is "hmac-sha1,hmac-sha256,hmac-sha512,hmac-md5,hmac-ripemd160,hmac-sha1-96,hmac-md5-96". If the connection is set to run in FIPS mode, the default is "hmac-sha1,hmac-sha256,hmac-sha512".

-o *option*

Sets any option that is supported in the configuration file (page 486). For example:

```
ssh "-o FIPSMode=yes" myuser@myhost
```

-p

Preserve time stamps and file attributes.

-P *port*

Port to connect to on the remote host.

-q

Enables quiet mode, which causes all warning and diagnostic messages, including banners, to be suppressed.

-Q

Turns off display of the progress indicator.

-R *maximum_requests*

Specifies the maximum number of concurrent requests. Increasing this may slightly improve file transfer speed but will increase memory usage. The default is 16 outstanding requests.

-s *subsystem*

Specifies the ssh subsystem.

-S *program*

Program to use for encrypted connections.

-u

Remove the source file after copying.

-v

Sets the debug level to verbose mode, which is equivalent to setting the debug level to 2.

-V

Displays product name and version information and exits. If other options are specified on the command line, they are ignored.

-4

Forces connections using IPv4 addresses only.

-6

Forces connections using IPV6 addresses only.

Interactive Mode

auto

Set transfer mode to automatic.

binary

Set transfer type to binary.

bye

Quit sftp.

cd *path*

Change remote directory to `path`.

chmod *path*

Changes the permissions associated with `path`. Use **mode** to specify a three digit numeric permissions.

lcd *path*

>Change local directory to `path`.

exit

>Quit **sftp**.

get *remote-path* [*local-path*]

>Retrieve the `remote-path` and store it on the local machine. If the local path name is not specified, it is given the same name it has on the remote machine.

getext [*extension*, *extension...*]

>Displays the file extensions that will use ascii transfer. Use **setext** to modify this list.

help

>Display help text.

lls [*ls-options* [*path*]]

>Display local directory listing of either `path` or current directory if `path` is not specified.

lmkdir *path*

>Create local directory specified by `path`.

lpwd

>Print local working directory.

ls [*path*]

>Display remote directory listing of either `path` or current directory if `path` is not specified.

mkdir *path*

>Create remote directory specified by `path`.

progress

>Toggle display of progress meter.

put *local-path* [*remote-path*]

>Transfers the `local-path` to the remote machine. If the remote path name is not specified, it is given the same name it has on the local machine.

pwd

>Display remote working directory.

quit

>Quit **sftp**.

reget *remote-file* [*local-file*]

>Resume the specified transfer. This works like the **get** command, but checks for the presence of a partially written local file and, if it is found, starts the transfer where the last attempt left off.

rename *oldpath newpath*

>Rename remote file from `oldpath` to `newpath`.

rmdir *path*

> Remove remote directory specified by `path`.

rm *paths*

> Delete remote file specified by `path`.

setext [*extension*, *extension...*]

> Sets the file extensions that will use ascii transfer. Wildcard characters are supported. When no argument is given, no file extensions use ascii transfer.

version

> Display **sftp** version.

?

> Synonym for **help**

ssh-keygen Command Line Utility

ssh-keygen - Creation, management, and conversion of keys used for client and server authentication.

Synopsis

```
ssh-keygen [-b bits] -t type [-N [passphrase]] [-C comment] [-f
output_keyfile]
ssh-keygen -B [-f input_keyfile]
ssh-keygen -c [-P passphrase] [-C comment] [-f keyfile]
ssh-keygen -e [-f input_keyfile]
ssh-keygen -p [-P old_passphrase] [-N new_passphrase] [-f keyfile]
ssh-keygen -i [-f input_keyfile]
ssh-keygen -y [-f input_keyfile]
ssh-keygen -l [-f input_keyfile]
```

Description

You can use the **ssh-keygen** command line utility to create RSA and DSA keys for public key authentication, to edit properties of existing keys, and to convert file formats. When no options are specified, **ssh-keygen** generates a 2048-bit RSA key pair and queries you for a key name and a passphrase to protect the private key. Public keys are created using the same base name as the private key, with an added `.pub` extension. The key location is displayed when key generation is complete.

Options

-b *bits*

> Specifies the key size. Up to a point, a larger key size improves security. Increasing key size slows down the initial connection, but has no effect on the speed of encryption or decryption of the data stream after a successful connection has been made. The length of key you should use depends on many factors, including: the key type, the lifetime of the key, the value of the data being protected, the resources available to a potential attacker, and the size of the symmetric key you use in conjunction with this asymmetric key. To ensure the best choice for your needs, we recommend that you contact your security officer. The default for ECDSA keys is 256 bits; DSA keys is 1024 bits; for RSA it is 2048 bits.

-B

Shows the fingerprint of the specified key in SHA-1 Bubble Babble format. You can specify the key file using **-f**. If you don't specify a file, you are queried for a filename. You can specify the private or public key name, but in either case, the public key must be available.

-C *comment*

Specifies information for the comment field within the key file. Use quotation marks if the string includes spaces. If you do not specify a comment when you create a key, a default comment is created that includes the key type, creator, date, and time.

-e

Uses the specified OpenSSH public or private key to generate a public key in Reflection format. You can specify the key file using **-f**. If you don't specify a file, you are queried for a filename.

-f *filename*

Specifies the filename for the generated private key. (A public key is also created and is always given the same name as the private key plus a `.pub` file extension.) This option can also be used in combination with **-e**, **-i**, **-l**, - **p**, **-y**, and **-B** to specify the input filename.

-i

Converts the specified Reflection public key to OpenSSH format. You can specify the key file using **-f**. If you don't specify a file, you are queried for a filename.

-h

Displays a summary of command line options.

-l

Show fingerprint of specified public key file using the MD5 hash. You can specify the key file using **-f**. If you don't specify a file, you are queried for a filename. If you specify a private key, **ssh-keygen** tries to find the matching public key file and prints its fingerprint.

-N *passphrase*

Sets the passphrase. For example, to specify the passphrase for a new key:

```
ssh-keygen -N mypassphrase -f keyfile
```

To create a new key that is not passphrase protected:

```
ssh-keygen -N -f keyfile
```

You can also use **-N** in combination with **-p** and **-P** to change the passphrase of an existing key.

-p

Use this option to change the passphrase of an existing private key. If you use this option alone, the program prompts for the file containing the private key, for the old passphrase, and twice for the new passphrase. You can use it in combination with **-f**, **-P**, and **-N** to change the passphrase non-interactively. For example:

```
ssh-keygen -p -f keyfile -P oldpassphrase -N newpassphrase
```

-P *passphrase*

Provides the (old) passphrase.

-q

> Silence **ssh-keygen**.

-t *type*

> Specifies the algorithm used for key generation. The possible values are "rsa" or "dsa" for protocol version 2.
>
> Possible values are "ecdsa", "rsa" or "dsa"

-y

> Uses the specified private key to derive a new copy of the public key. You can specify the key file using **-f**. If you don't specify a file, you are queried for a filename.

Return values

> **ssh-keygen** returns 0 (zero) if the command completes successfully. Any non-zero value indicates a failure

scp Command Line Utility

Syntax: scp [options] [user@host:]file1 [user@host:]file2

The **scp** command line utility copies files securely between hosts on a network. It uses Secure Shell **sftp** subsystem for data transfer, and uses the same authentication and provides the same security as Secure Shell. **Scp** will ask for passwords or passphrases if they are needed for authentication. Any file name may contain a host and user specification to indicate that the file is to be copied to/from that host.

Examples

This command line copies the file `f1` from the host to the local machine and gives it the name `f2`:

```
scp user@host:f1 f2
```

This command copies the local file `f1` to `f2` on the remote host.

```
scp f1 user@host:f2
```

NOTE: You can reuse an existing Secure Shell connection. However, to do so you must explicitly enable this on each command line, or set the SSHConnectionReUse environment variable to Yes. For details, see .

Options

The following options are available:

-a

> Transfer files in ASCII mode.

-b *buffersize*

> Sets the maximum buffer size for one request.

-B

Sets batch mode on, which prevents asking for passwords or passphrases. Use passphraseless user keys to authenticate.

-c *cipher*

A comma-separated list of ciphers specified in order of preference. The default is "aes128-ctr,aes128-cbc,aes192-ctr,aes192-cbc,aes256-ctr,aes256-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour128,arcfour256,arcfour".

Protocol version 1 (which is deprecated and not recommended) allows specification of a single cipher. The supported values are "3des", "blowfish", and "des".

-C

Enable compression.

-d

Force target to be a directory.

-D *level*

Sets the debug level. Allowed values are 1,2, and 3.

-F *configfile*

Specifies an alternative per-user configuration file (page 484). If a configuration file is given on the command line, the system-wide configuration file will be ignored.

-h

Displays a summary of command line options.

-H *scheme*

Specifies which SSH configuration scheme (page 485) to use for this connection.

-i *keyfile*

Selects a file from which the identity (private key) for RSA or DSA authentication is read. Identity files may also be specified on a per-host basis in the configuration file. It is possible to have multiple **-i** options (and multiple identities specified in a configuration file (page 485)). Path names containing spaces must be embedded inside double quotation marks.

-k *directory*

Specifies an alternate location for the config, host key, and user key files. Note: When -k is used, host keys are read and written from the specified location only if a known-hosts file already exists in that location. If no known-hosts file is found, host keys are read and written to the known-hosts file in the default location.

-o *option*

Can be used to give options in the format used in the configuration file (page 485). This is useful for specifying options for which there is no separate command-line flag. For a list of supported options, see the Configuration Keyword Reference (page 486).

--overwrite

Specifies whether or not to overwrite existing destination files. The allowed values are 'yes' and 'no'. The default is 'yes'.

-p

Preserve timestamps and file attributes.

-P *port*

Port to connect to on the remote host.

-q

Quiet mode. Causes all warning and diagnostic messages, including banners, to be suppressed.

-Q

Turns off display of the progress indicator.

-r

Copy directories recursively, including all subdirectories.

-u

Remove the source file after copying.

-v

Verbose mode. Causes `ssh` to display debugging messages about its progress. This is helpful in debugging connection, authentication, and configuration problems. Multiple **-v** options increases the verbosity. Maximum is 3 (-vvv).

-V

Display the version number and application information.

-z

By default filename matches are case-sensitive for all downloads. With this option, downloads that include wildcards in the server filename specification are not case-sensitive.

-1

Forces protocol version 1 only. This option also transfers file to OpenSSH servers using rcp through the ssh tunnel.

-2

Forces protocol version 2 only.

-4

Use only IPv4 addresses.

-6

Use only IPv6 addresses

Troubleshooting Secure Shell

In this Section

Troubleshooting Secure Shell Connections

If you are having trouble making a Secure Shell connection the trouble may come because Reflection cannot locate your host, or because of a problem with either host authentication or user authentication.

Using log files

If your connection problem is with host authentication (page 442), you may find useful information in the Reflection client log file (page 519).

If your problem is with user authentication (page 445), you may need to contact the administrator of the Secure Shell server. User authentication problems are common, and complete information about failed user authentication is available only in the server debug log-not in the client log. By design, the Secure Shell protocol does not provide specific information to clients about failed authentication attempts. This is done so that an attacker cannot use error messages to determine why an authentication failed and thus narrow in on a successful attack.

Troubleshooting suggestions

Password authentication

◆ Incorrect password. Check that Caps lock is not enabled.

◆ Expired password. You may need to use Keyboard Interactive authentication instead of Password authentication to enable password updates.

◆ If no password prompt is displayed, password authentication may be disabled.

Public Key authentication

◆ User's public key has not been uploaded to the correct location on the host.

◆ User's public key has been uploaded to the correct location but has incorrect ownership or file permissions.

◆ Key is passphrase protected and you have entered an incorrect passphrase.

◆ The wrong key is selected for authentication on the User Keys (page 472) tab of the Secure Shell Settings dialog box.

◆ Too many public keys are selected, especially if you are attempting connections to servers running older versions of OpenSSH.

Certificate authentication

◆ The certificate used to authenticate the host is not available. Check the Reflection trusted root store and the Microsoft trusted root and intermediate stores. (If use of the Microsoft store has been disabled, certificates must be in the Reflection store.)

◆ The certificate used to authenticate the user is not available. Check the Reflection personal store and the Microsoft personal store.

◆ The certificate used to authenticate either the host or user has expired.

◆ Certificate host name must match host being contacted (page 479) is enabled and the host name you have specified for this connection doesn't exactly match host name in certificate.

- Certificate revocation checking is enabled (page 479) and the Certificate Revocation List is not available.
- Certificate revocation checking is enabled (page 479) and the host certificate has been revoked.

Key exchange

- The following error occurs during key exchange: "fatal: dh_gen_key: group too small: 1024 (2*need 1024)". Modify the key exchange algorithms to put diffie-hellman-group14-sha1 ahead of the other algorithms.

Related Topics

- "Enabling and Disabling Use of the Windows Certificate Store" on page 521

Use the Secure Shell Log File

The log file contains information you can use to troubleshoot Secure Shell connections.

NOTE: You can use the Logging Level setting to determine the amount of information written to the Secure Shell log. This setting is available from the Reflection Secure Shell Settings dialog box -- General tab (page 469).

To use the log file from the Reflection workspace

1 Capture a trace.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Tools**tab, in the **Tracing**group, click **Start Trace.**Then perform the actions to trace. In the **Tracing**group, choose **Stop Trace**, and then choose **Process Trace**.
Reflection Browser	On the **Reflection** menu choose **Tools, Trace**, and then **Start Trace**. Then perform the actions to trace. On the **Reflection** menu choose **Tools, Trace**, and then **Stop Trace**. In the search box, enter P and then, under **Actions**, select **Process Trace**.
TouchUx	On the menu, select the Wrench icon and then, under **Trace**, select **Start Trace**. After you have performed the actions to trace, select the Wrench icon and choose **Stop Trace.**Then select the Wrench icon again and choose **Process Trace**.

2 Select **Network protocol details**, and then click **OK**.

3 Locate the event file (*.rev) and then click **Open**.

4 Select a filename and format for your log output, and then click **Save**.

To use the log file from the FTP Client

- Do one of the following:

To	Choose
Send log information to a file	**Tools** > **Start Logging,** and then change **Files of Type** to "Diagnostic File (*.txt)".
View the log information in the FTP command window	**View** > **Command Window**.

Certificate Authentication (PKI)

In this Section

PKI and Certificates

A Public Key Infrastructure (PKI) is a system that helps facilitate secure communications through the use of digital certificates. You can use of a PKI for both host and user authentication.

Like public key authentication, certificate authentication uses public/private key pairs to verify the host identity. However, with certificate authentication, public keys are contained within digital certificates, and in this case, two key pairs are used. For example, for server authentication, the host holds one private key and the CA holds a second. The host obtains a certificate from the CA. This certificate contains identifying information about the host, a copy of the host public key, and a digital signature created using the CA's private key. This certificate is sent to the client during the authentication process. To verify the integrity of the information coming from the host, the client must have a copy of the CA's public key, which is contained in the CA root certificate. There is no need for the client to have a copy of the host public key.

Certificate authentication solves some of the problems presented by public key authentication. For example, for host public key authentication, the system administrator must either distribute host keys for every server to each client's known hosts store, or count on client users to confirm the host identity correctly when they connect to an unknown host. When certificates are used for host authentication, a single CA root certificate can be used to authenticate multiple hosts. In many cases the required certificate is already available in the Windows certificate store.

Similarly, when public keys are used for client authentication, each client public key must be uploaded to the server and the server must be configured to recognize that key. When certificate authentication is used, a single CA root certificate can be used to authenticate multiple client users.

Certificate stores

Digital certificates are maintained on your computer in certificate stores. A certificate store contains the certificates you use to confirm the identity of remote parties, and may also contain personal certificates, which you use to identify yourself to remote parties. Personal certificates are associated with a private key on your computer.

You can use digital certificates located in either or both of the following stores:

- **The Windows Certificate Store**

  This store can be used by a number of applications, web browsers, and mail clients. Some certificates in this store are included when you install the Windows operating system. Others may be added when you connect to internet sites and establish trust, when you install software, or when you receive an encrypted or digitally signed e-mail. You can also import certificates manually into your Windows store. Manage the certificates in this store using the Windows Certificate Manager.

- **The Reflection Certificate Store**

  This store is used only by Micro Focus applications. To add certificates to this store, you must import them manually. You can import certificates from files and also use certificates on hardware tokens such as smart cards. Manage the certificates in this store using the Reflection Certificate Manager.

You can configure authentication to use only those certificates located in Reflection Certificate Manager store, or using both the Windows and the Reflection Certificate Manager store. Enabling host authentication using the Windows certificate store means that you may not need to import certificates, because authentication may be accomplished using certificates that are already available. Disabling authentication using the Windows certificate store enables you to have greater control over which certificates are used for authentication. To enable or disable authentication with the Windows Certificate store, open the Reflection Certificate Manager and click the **Trusted Certificate Authorities** tab.

PKI in Terminal and FTP Client sessions

PKI authentication is supported in both Secure Shell and SSL/TLS sessions.

- All SSL/TLS sessions require certificates for host authentication; without the necessary certificate, you cannot make a host connection. Depending on the host configuration, you may also need to install certificates for user authentication.

- Secure Shell sessions typically require both host and user authentication. Certificates can be used for either host and/or user authentication, but are not required by default

Enabling and Disabling Use of the Windows Certificate Store

Reflection Secure Shell and SSL/TLS sessions support the use of digital certificates (page 897) for both host and user authentication. Reflection applications can be configured to authenticate using only those certificates located in Reflection store, or using both the Windows and the Reflection store.

Host authentication

Enabling use of the Windows certificate store means that you may not need to import the certificates used for host authentication. If your host certificates were acquired from a well-known Certification Authority (page 897) (CA), such as VeriSign or Thawte, a certificate identifying the issuer as a trusted CA should already be included in the Trusted Root Certification Authorities list on your system. When use of the system store is enabled, Reflection clients look for certificates in both the Reflection and the system store.

Disabling use of the Windows certificate store enables you to have greater control over which certificates are used for authentication. Certificates can be added to the Windows store in a variety of ways, and you may not want to allow use of all of these certificates for authenticating Reflection sessions. When use of the Windows store is disabled, only those certificates you have imported into the Reflection store are used for host authentication.

To enable (or disable) host authentication using certificates in the Windows store:

1   Open the "Reflection Certificate Manager" on page 528.

2   Click the **Trusted Certificate Authorities (page 531)** tab.

3   Select (or clear) **Use System Certificate Store for SSH connections** and/or **Use System Certificate Store for SSL/TLS connections**.

User authentication

Reflection uses personal certificates in the Windows store and the Reflection store in the same way. Available personal certificates include those in the Windows personal store, the Reflection personal store (page 530), and certificates on configured hardware tokens (page 535) (for example smart cards).

   ◆ If you have configured a Reflection Secure Shell session, you must specify which certificates to use for user authentication from the **User Keys** tab in the Secure Shell settings dialog box.

   ◆ If you have configured a Reflection SSL/TLS session, all certificates located in either store are automatically available for user authentication.

Configuring Certificate Revocation Checking

Reflection SSL/TLS and Secure Shell connections can be configured to authenticate hosts using digital certificates (page 897). To ensure that certificates have not been revoked, you can configure Reflection to check for certificate revocation using CRLs (page 897) or using an OCSP (page 898) responder.

When CRL checking is enabled, Reflection always checks for CRLs in any location specified in the CRL Distribution Point (CDP) field of the certificate. In addition, Reflection can also be configured to check for CRLs located in an LDAP (page 898) directory or using an OCSP (page 898) responder.

Reflection's default value for certificate revocation checking is based on your current system setting. If your system is configured to do CRL checking, all Reflection sessions will check for certificate revocation using CRLs by default.

NOTE: When Reflection is running in DOD PKI mode (page 524), certificate revocation is always enabled and cannot be disabled.

To enable CRL checking for all SSH sessions

1 In Internet Explorer, choose **Tools** > **Internet Options** > **Advanced**.

2 Under **Security**, select **Check for server certificate revocation**.

Using Reflection, you can enable certificate revocation checking using either a CRL or an OCSP responder.

To enable CRL checking for a Secure Shell session

1 Open the **Reflection Secure Shell Settings** dialog box.

2 Click the **PKI** tab.

3 Select either **Use OCSP** or **Use CRL**.

To enable CRL checking for SSL/TLS sessions

1 Open the **Security Properties (page 542)** dialog box.

2 On the **SSL/TLS** tab, click Configure PKI. (**Use SSL/TLS security** must be selected.)

3 Select either **Use OCSP** or **Use CRL**.

NOTE: CRLs and/or OCSP responders required by a certificate are identified in the AIA and/or CDP extension of the certificate. If this information is not provided in the certificate, you can use the **OCSP (page 534)** and **LDAP (page 533)** tabs of the Reflection Certificate Manager to configure it.

Distributing Intermediate Certificates using an LDAP Directory

Reflection SSL/TLS and Secure Shell connections can be configured to authenticate hosts using digital certificates (page 897). Depending on how you have configured the Reflection Certificate Manager (page 521), Reflection may use certificates in just the Reflection store or in both the Windows and Reflection stores. The Windows store holds intermediate as well as trusted root certificates. The Reflection store holds trusted root certificates only. Reflection can also be configured to locate intermediate certificates from an LDAP server.

To configure Reflection to locate intermediate certificates stored in an LDAP directory, use the **LDAP (page 533)** tab of the Reflection Certificate Manager to identify the LDAP server (or servers).

Configuring the LDAP server

Reflection can locate a certificate in the LDAP directory only if the LDAP distinguished name (DN) exactly matches the contents of the Subject field in the certificate. For example, if the Subject field of the certificate displays the following objects:

- CN = Some CA
- O = Acme
- C = US

The DN of the entry in the LDAP directory must be exactly: "CN = Some CA, O=Acme, C = US".

The attributes of the LDAP entry identified by this DN must include one of the following. (Reflection looks for these attributes in order from top to bottom.)

Attribute	OID (Object Identifier)
userCertificate;binary	2.5.4.36
cACertificate;binary	2.5.4.37
userCertificate	2.5.4.36
cACertificate	2.5.4.37
mosaicKMandSigCertificate	2.16.840.1.101.2.1.5.5
sdnsKMandSigCertificate	2.16.840.1.101.2.1.5.3
fortezzaKMandSigCertificate	2.16.840.1.101.2.1.5.5
crossCertificatePair;binary	2.5.4.40
crossCertificatePair	2.5.4.40

DOD PKI Information

This section describes how to install, configure, and use Reflection to operate within the Department of Defense (DOD) or other Public Key Infrastructure (PKI) (page 520) environment. PKI configuration affects both Secure Shell and SSL/TLS connections.

Running Reflection in DOD PKI mode

By default, Reflection applications allow some configurations that do not meet DOD PKI requirements. Administrators can use Reflection Group Policies to configure all Reflection sessions to meet DOD PKI requirements.

To configure DOD PKI mode

1 Run the Group Policy Editor using one of the following techniques:

   ◆ On the command line, enter `Gpedit.msc`

     –or–

   ◆ In the Active Directory Users and Computers console, open the properties for an Organizational Unit, click the **Group Policy** tab, and edit or create a new policy object.

2 Install the Reflection template (ReflectionPolicy.adm) if you have not already done so.

   NOTE: For information about how to download and install the Reflection policy template, see Knowledge Base Article 7021501 (https://support.microfocus.com/kb/doc.php?id=7021501).

3 Under **Local Computer Policy** > **User Configuration** > **Administrative Templates** > **Reflection Settings**, disable the setting **Allow non-DoDPKI mode**.

Configuring DOD PKI mode has the following effects.

   ◆ You must configure Reflection to use either CRL (page 897) checking or an OCSP (page 898) responder. In DOD PKI mode, the option to use neither form of checking is disabled. (For SSH connections, certificate revocation is configured using the PKI tab of the Secure Shell settings dialog box. For SSL/TLS connections it is configured using the PKI Configuration dialog box.)

- Reflection enforces FIPS-approved encryption algorithms. For SSH connections, this means that only FIPS-approved options are available on the Encryption tab of the Secure Shell settings dialog box.

- For a connection to succeed, the certificate host name must exactly match the host name specified for your Reflection connection. This means that the setting **Certificate must match host name being contacted** is automatically selected and cannot be modified. (For SSH connections, this setting is configured using the **PKI (page 479)** tab of the **Reflection Secure Shell Settings** dialog box. For SSL/TLS connections it is configured using the **PKI Configuration (page 547)** dialog box.)

- Intermediate CA certificates signed using the MD2 or MD5 hash are not supported for certificate validation.

Installing and Removing Trust Points

A trust point is any CA (page 897) certificate in a chain of trust.

To add a trust point to the Reflection certificate store:

1. Open the Reflection Certificate Manager (page 529).

2. Click the **Trusted Certificate Authorities** tab.

3. Click **Import**, then browse to locate a certificate (typically *.cer or *.crt).

To remove a trust point from the Reflection certificate store,

1. Open the Reflection Certificate Manager (page 529).

2. Click the **Trusted Certificate Authorities** tab.

3. Select the certificate and click **Remove**.

NOTE

- Intermediate CA trust points can be retrieved from an LDAP (page 898) or HTTP server which may be identified by explicit URIs defined in the Authority Information Access (AIA) extension of a certificate, or using LDAP server information configured on the LDAP tab of the Reflection Certificate Manager. These certificates are stored in the cert_cache file located in either `<My Documents>\Micro Focus\Reflection\.pki` or `\%programdata%\Micro Focus\Reflection\.pki`

- When Reflection is running in DOD PKI mode, only those root certificates you have added to the Reflection Certificate manager are used. There is no need to remove any non-DOD PKI certificates that may be present in the Windows Certificate Store.

Configuring Certificate Revocation Checking

Reflection's default value for certificate revocation checking is based on your current system setting. If your system is configured to do CRL checking, Reflection sessions will check for certificate revocation using CRLs (page 897) by default. You can also configure Reflection to use an OCSP (page 898) responder.

Reflection also supports a setting to disable CRL checking. You may want to use this setting for testing purposes, however this option is not available if Reflection is running in DOD PKI mode.

CAUTION: Disabling CRL checking compromises your security. Use this option only for testing purposes.

You can define one or more LDAP (page 898) servers from which to retrieve intermediate certificates or CRLs.

To define an LDAP server

1 Open the Reflection Certificate Manager (page 529)

2 Click the **LDAP** tab.

3 Click **Add**, then specify the server using the following URL format:

```
ldap://hostname:portnumber
```

For example:

```
ldap://ldapserver.myhost.com:389
```

To configure OCSP

1 You can define one or more OCSP servers from which to request certificate revocation information.

2 Set **Certificate Revocation** to **Use OCSP**. (For SSH connections use the PKI tab of the Secure Shell settings dialog box. For SSL/TLS connections use the PKI Configuration dialog box.)

NOTE: OCSP responder URLs required by a certificate are identified in the AIA extension of the certificate. If this information is not provided in the certificate, you can use the following steps to configure OCSP responder information.

3 Open the Reflection Certificate Manager (page 529).

4 Click the **OCSP** tab.

5 Click **Add**, then specify the server using the following URL format:

```
URL:portnumber
```

For example:

```
https://ocspmachine.host.com:389
```

Using Uniform Resource Identifiers for DOD PKI Services

Reflection supports the use of URIs (page 900) for automatic CRL (page 897) updating and retrieval. As defined in section 4.2.1.14 of RFC3280.

If CRL checking is enabled, Reflection checks for certificate revocation as follows:

1. Check the crl_cache file for valid revocation information. If none is found, continue on to step 2.

2. Check the CDP extension in the certificate for HTTP or LDAP URIs and query these in the order specified (first HTTP, then LDAP). If the certificate is found to be revoked, close the connection. If the certificate is not found continue on to step 3.

3. If one or more LDAP servers is specified in the Reflection Certificate Manager LDAP tab, assemble the Distinguished Name for the CA listed in the Issuer extension of the certificate and query for the CRL file. If the certificate is not found to be revoked in any CRL, continue to the next validation step.

Updates for expired CRLs are handled automatically, and do not require administrator intervention or configuration.

If OCSP checking is enabled, Reflection always checks all available OCSP responders to ensure that the connection will fail if any of these responders knows that the certificate has been revoked. For the connection to succeed at least one OCSP responder must be available and return a value of 'good' for the certificate status. Reflection performs these checks as follows.

1. Check the AIA extension in the certificate for one or more OCSP responders and query each of those responders. If the status of the certificate comes back as 'revoked' from any responder, close the connection.

2. Check for one or more user configured OCSP responders specified using the Reflection Certificate Manager OCSP tab and query each of those responders. If the status of the certificate comes back as 'revoked' from any responder, close the connection.

3. If all responders returned 'unknown' close the connection. If a 'good' response was returned from at least one of the queried OCSP responders continue on to the next validation step.

Using URIs to Retrieve Intermediate Certificates

As defined in section 4.2.2.1 of RFC3280, Reflection can use URIs (page 900) to retrieve intermediate CA (page 897) certificates as follows:

1. Check the cert_cache file for the required intermediate certificate. If it is not found, continue on to step 2.

2. If either HTTP or LDAP URIs are defined in the Authority Information Access (AIA) extension of a certificate, attempt to use these (first HTTP, then LDAP) to retrieve intermediate CA certificates.

3. If the preceding attempts fail, assemble a Distinguished Name from the issuing certificate's Subject Name, and queries the defined LDAP server for the contents of the CACertificate attribute.

Because Reflection does not enforce the security policy extension of a certificate, security policy configuration is not necessary.

Configuring and Protecting Certificates and Private Keys

To configure client authentication using certificates:

1 "Open the Reflection Certificate Manager" on page 529

2 On the **Personal** tab, click **Import**, then browse to locate a certificate (typically *.pfx or *.p12). You will be prompted to create a passphrase that will be required any time this key is used. Entering a passphrase is advisable to help protect this key on your system.

3 For Secure Shell connections, open the **Reflection Secure Shell Settings** dialog box, click the **User Keys** tab and select the certificate(s) you want to use for client authentication to the currently specified host. (This step is not required for SSL/TLS connections.)

Private Key Safeguards

If a client private key is stolen, a malicious user can gain access to files on any servers accessible to that user. To minimize this risk, each client user should always protect his or her private key with a passphrase. This ensures that only someone who knows the passphrase can authenticate with that key. Users should create and protect passphrases following the password specifications in your organization's Security Policy.

Actions to Take if a Key is Compromised

Consider a private key compromised if it has become available to any unauthorized entity, or if you have reason to distrust the actions of any person who has access to the key.

If the client key is compromised, revoke the client certificate.

To replace a compromised key:

1 Generate a new private key and certificate and import the key into the Reflection Certificate Manager.

2 On the server, update the map file line for this client if the identifying information has changed.

To remove the compromised key from the client computer:

1 Remove the key from the **Personal** (page 530) tab of the Reflection Certificate manager. This removes this key from the identity_store.p12 file.

2 If the original file containing the old key and certificate (*.pfx or *.p12) is still on the client computer, use a DOD-approved file erasure utility to delete this file.

Related Topics

Reflection Certificate Manager

Use Reflection Certificate Manager to manage the digital certificates in the Reflection Certificate Manager certificate store and to configure other aspects of PKI support.

Certificate authentication can use certificates located in either the Windows certificate store or the Reflection Certificate Manager store (or both). The Reflection Certificate Manager store can be used for authentication during Secure Shell and/or SSL/TLS sessions.

Open the Reflection Certificate Manager

NOTE: The procedures for opening the Certificate Manager depend on your product and session type. Your product may support one or more of the following procedures.

From the Secure Shell Settings dialog box

1 Open the Reflection Secure Shell Settings dialog box.

2 On the PKI tab, click Reflection Certificate Manager.

From the Security Properties dialog box

1 Open the Security Properties dialog box.

2 On the SSL/TLS tab, select Use SSL/TLS Security.

3 Click Configure PKI.

4 Click Reflection Certificate Manager.

From the TCP/UDP Path Options dialog box

1 Set Security type to something other than No Security.

2 Click PKI Settings.

3 Click Reflection Certificate Manager.

Opening the Windows Certificate Manager from Internet Explorer

1 Open Microsoft Internet Explorer.

2 On the Tools menu, click Internet Options.

3 On the Content tab, click Certificates.

Opening the Windows Certificate Manager from the Control Panel

1 Use the Windows Start menu to open the Control Panel.

2 Double-click Internet Options.

3 On the Content tab, click Certificates.

Opening the Windows Certificate Manager from a terminal session

While you are configuring your terminal sessions, you can access the Windows Certificate Manager from either the Secure Shell Settings dialog box or the Security Properties dialog box. Availability of these dialog boxes depends on the application and security protocol you are using.

From the Secure Shell Settings dialog box

1 Open the Reflection Secure Shell Settings dialog box.

2 On the PKI tab, click View System Certificates.

From the Security Properties dialog box

1 Open the Security Properties (page 542) dialog box.

2 On the SSL/TLS tab, select Use SSL/TLS Security.

3 Click Configure PKI.

4 Click View System Certificates.

Server Certificate not Found

The host is presenting a self-signed server certificate that is not in the Trusted Root Certification Authorities list of your Window's certificate store.

The options are:

Always	Accept the certificate and add it to your trusted root list. The host will be authenticated with this certificate in subsequent connections and this dialog box will not appear again unless the certificate is removed from the list.
	NOTE: The accepted certificate is saved to your user-specific certificate store. If your system administrator has configured a global certificate store, certificates in your personal store are not used and you will continue to see this prompt.
Once	Accept the certificate for this connection only, but don't load it into the certificate store.
No	Decline the certificate and close the connection.

CAUTION: Accepting a self-signed certificate can create a security risk. The appearance of this dialog box might be the result of a "man-in-the-middle attack," in which another server poses as your host. If you are not sure how to respond, click **No** and contact a system administrator.

Personal Tab (Reflection Certificate Manager)

Use this tab to manage the personal certificates in the Reflection Certificate Manager store. Personal certificates are used for user (client) authentication.

The options are:

Import	Add a certificate to the Reflection Certificate Manager store. The imported file (typically a *.pfx or *.p12) must include a private key. Depending on how the file was created, you may be prompted for a password before you can import the file.
	You will be prompted to enter a passphrase to protect the private key. If you specify a passphrase, you'll be prompted for this passphrase when this certificate is used to authenticate to a host.
Remove	Remove the selected certificate.
View	View the selected certificate.
Change Passphrase	Change the passphrase for the selected certificate.

Trusted Certification Authorities Tab (Reflection Certificate Manager)

Use this tab to manage certificates from trusted certification authorities (CAs) in the Reflection Certificate Manager store. Micro Focus applications that support the Reflection Certificate Manager automatically use any certificates in the Trusted Certification Authorities store for host (server) authentication.

Import	Add a certificate (typically *.cer or *.crt) to the store.
Remove	Remove the selected certificate from the store.
View	View the selected certificate.
Store trusted certificates in the common application data folder	By default, trusted roots that you add using the Import button are saved to the following file, which makes them available only to your current user account:

personal_documents_folder `\Micro Focus\Reflection\.pki\trust_store.p12`

For example:

`\Users\username\Documents\Micro Focus\Reflection\.pki\trust_store.p12`

Select **Store trusted certificates in the common application data folder** to import a certificate to the following location, which makes it available to all users of the computer:

`%programdata%\Micro Focus\Reflection\.pki\trust_store.p12`

NOTE

- The value of this setting is not saved. Selecting or clearing it only affects which certificate store you are viewing and editing while the dialog box remains open. If a shared store is present, this setting is selected by default when you open the dialog box. If no shared store is present, the setting is not selected by default.

- If a shared store exists, trusted roots are read exclusively from the shared store. Trusted roots you have configured for individual user accounts no longer have any effect.

- To revert to user-specific trusted root stores after creating a shared store, you must delete or rename the shared `trust_store.p12` file. If you simply clear this setting, subsequent changes will modify your personal store, but the personal store continues to have no effect as long as `trust_store.p12` is still present in the common application data folder.·

- If the operating system has been configured by the administrator to deny users write access to `\%programdata%\Micro Focus\Reflection`, this setting is not available to those users and they will not be able to modify items in the shared trusted root store.

Use System Certificate Store for SSH connections	When this item is selected, your application uses certificates in your Windows certificate store (in addition to any certificates you have imported into the Reflection Certificate Manager store) to authenticate hosts when establishing a Secure Shell connection.
	Clear this setting to ensure that your sessions authenticate hosts using only the certificates in the Reflection Certificate Manager store.
Use System Certificate Store for SSL/ TLS connections	When this item is selected, your application uses certificates in your Windows certificate store (in addition to any certificates you have imported into the Reflection Certificate Manager store) to authenticate hosts when establishing an SSL/TLS connection.
	Clear this setting to ensure that your sessions authenticate hosts using only the certificates in the Reflection Certificate Manager store.
Allow MD5 signed certificates **Allow MD2 signed certificates**	When these items are selected, validation allows intermediate CA certificates signed with the specified hash. When these items are not selected, certificate validation fails if an intermediate certificate is signed with the specified hash.

   - These certificate hash settings affect intermediate CA certificates only; any certificate that has been added to your trusted root store is trusted, regardless of the signature hash type.
   - These settings are not available if your application has been configured by group policy to run in DOD PKI mode.

LDAP Tab (Reflection Certificate Manager)

The Lightweight Directory Access Protocol (LDAP) is a standard protocol that can be used to store information in a central location and distribute that information to users. Administrators can configure an LDAP server to distribute information needed by users who are authenticating with certificates. This information can include:

   - Certificate Revocation Lists (CRLs), which are used to ensure that certificates being used have not been revoked by the certification authority.
   - Intermediate certificates needed to establish a valid certification path from the server certificate to a trusted root certification authority.

Use the LDAP tab of the Reflection Certificate Manager to list LDAP servers that distribute this information. The options are:

Add	Add an LDAP server to the list. Specify the server using the following URL format:
	
	`ldap://hostname[:portnumber]`
	
	For example:
	
	`ldap://ldapserver.myhost.com:389`

Modify	Edit the server URL.
Remove	Remove the selected server from the list.

NOTE

- It is not necessary to configure an LDAP server to use CRL checking. When CRL checking is enabled, validation includes CRLs in any location specified in the CRL Distribution Point (CDP) field of the certificate. Configuring an LDAP server provides an additional mechanism for retrieving CRL lists.
- Server URLs that use the LDAPS scheme (for example, ldaps://hostname:port) to transfer LDAP data using SSL are not supported.

Configuring the LDAP Server for CRL Checking

A CRL in the LDAP directory can only be located if the LDAP distinguished name (DN) exactly matches the contents of the Issuer field in the CRL. For example, if the Issuer field of the CRL displays the following objects:

- CN = Some CA
- O = Acme
- C = US

The DN of the entry in the LDAP directory must be exactly: "CN = Some CA, O=Acme, C = US".

The attributes of the LDAP entry identified by this DN must include one of the following. (These attributes are searched for in order from top to bottom.)

Attribute	OID (Object Identifier)
certificateRevocationList;binary	2.5.4.39
authorityRevocationList;binary	2.5.4.38
certificateRevocationList	2.5.4.39
authorityRevocationList	2.5.4.38
deltaRevocationList;binary	2.5.4.53
deltaRevocationList	2.5.4.53
mosaicCertificateRevocationList	2.16.840.1.101.2.1.5.45
sdnsCertificateRevocationList	2.16.840.1.101.2.1.5.44
fortezzaCertificateRevocationList	2.16.840.1.101.2.1.5.45

OCSP Tab (Reflection Certificate Manager)

Getting there (page 529)

Configure one or more OCSP responders for certificate revocation checking. Click **Add** to add a server to the list. By default, every server you add is queried for certificate validity, starting with the first server on the list. Clear the check box next to a server to disable certificate checking for that server without removing the server from the list.

Add   Add an OCSP server to the list. Specify the server using the following URL format:

`URL:portnumber`

For example:

`www.ocspresponder.com:80`

Modify   Edit the server URL.

Remove   Remove the selected server from the list.

PKCS#11 Tab (Reflection Certificate Manager)

Getting there (page 529)

Use the PKCS#11 tab to configure authentication using hardware devices, such as smart cards or USB tokens. Your hardware device must conform to PKCS#11 specifications.

This tab displays all currently available devices, and any certificates or public keys located on those devices. When use of a device is enabled using the check box provided, any certificates or keys on the device are used automatically for user authentication.

You must install the software supplied by your token provider before you can configure your Micro Focus application to authenticate using a hardware token. To configure authentication using the token, you will also need to know the name and location of the library file (*.dll) used by that provider to provide access to your hardware device.

The options are:

Providers list	Displays devices currently available. Clear the check box(es) to disable authentication with a listed device.
Device Contents	Displays keys and certificates available on the selected device.
View Certificate	Displays the selected certificate.
Disconnect automatically when token is removed	When selected, the connection is active only while the token is present.
Seconds to wait before disconnecting	Specifies the number of seconds to wait to disconnect after a token is removed.

Related Topics

◆ "PKCS#11 Provider Dialog Box" on page 536

PKCS#11 Provider Dialog Box

Getting there (page 529)

The options are:

Provider DLL	Specify the file name and location of the library used to access the hardware device. This is typically installed to the Windows system folder. You may need to contact the device manufacturer to determine the correct file.
Slots	Identify the card slot that holds the card being used for authentication.
Additional parameters	Specify any additional parameters needed to access the information on the hardware device.

Related Topics

◆ "PKCS#11 Tab (Reflection Certificate Manager)" on page 535

SOCKS or HTTP

You can configure sessions to connect through a SOCKS proxy server or an HTTP server.

NOTE: SOCKS and HTTP are supported for VT, IBM 3270, and IBM 5250 terminals.

Related Topics

◆ "Security Properties Dialog Box" on page 542

SOCKS Overview

SOCKS is a software protocol used in conjunction with a firewall host system to provide secure, controlled access to internal and external networks. When you request a network connection from a SOCKS-enabled application, the SOCKS Client software communicates with the SOCKS server software to determine if the connection is allowed. If it is, the connection is established. If it is not, the SOCKS server rejects the connection request.

To enable SOCKS support, use the **SOCKS** tab of the **Security Properties** dialog box (or, if you are also configuring a Secure Shell connection, use the **Reflection Secure Shell Settings** dialog box). After enabling SOCKS support, you must configure the SOCKS client. You can configure the software in one of two ways: designate a single SOCKS proxy server through which all requested connections must pass; or designate specific SOCKS proxy servers (or request that the SOCKS proxy server be bypassed) for specific destination addresses.

When the SOCKS protocol is enabled and you use a Reflection application to request a connection to a remote host, Reflection determines if the connection request must go through the firewall system. If the firewall system must be used, the application uses the SOCKS protocol to communicate with the SOCKS server software, which determines if the connection is allowed.

The Reflection SOCKS Client is compliant with SOCKS version 4 and works with SOCKS version 4 or version 5 servers.

NOTE: If your SOCKS server requires authentication before it will grant a connection request, you must run the Identification Daemon. The Identification Daemon (IdentD) authenticates TCP connections between two hosts. Some SOCKS servers require authentication before they will grant a connection request through the firewall. The Identification Daemon must be running to perform this authentication.

Check with your system administrator to determine whether your SOCKS proxy server requires identification (that is, whether the SOCKS daemon was started using the -i or -I option). If the server does not require authentication, the Identification Daemon has no effect on SOCKS. The Identification Daemon has no configurable options.

Related Topics

 ◆ "Security Properties Dialog Box" on page 542

Socks Configuration Dialog Box

Getting there

1 In the Security Properties dialog box, on the **Proxy**tab, click **Use proxy server**.

2 Under **Proxy type**, select **SOCKS**and then click **Configure**.

Use this dialog box to designate SOCKs proxy servers. You can designate a single SOCKS proxy server through which all requested connections must pass or use Advanced options to designate multiple SOCKS proxy servers.

SOCKS proxy

Enter information to designate a single SOCKS proxy server. If you want to configure more than one proxy server or configure specific destination routes, leave the fields in the SOCKS proxy group blank and click Advanced.

Server address	Type the SOCKS proxy server address in this box.
Protocol version	Choose the protocol version your server uses from the menu.
Advanced	Click to configure multiple SOCKS proxy servers and destination routing filters for connection requests (see the following Advanced options).

Advanced options

Configure multiple proxy servers in order of preference. When a connection is requested, the client attempts to match the request with these addresses, beginning at the top of the list and moving down. The final line in the list, "Any address on any port", serves as a match for any request and prevents a connection request from being ignored.

To bypass a proxy server, select it from the list of destinations, click **Change**, and select the **Do not use...** check box.

Destination	Specifies the name or IP address as well as the port number of one or more destination hosts. (Asterisks in an IP address represent wildcard characters.)
Proxy	Specifies the name or IP address of the proxy server associated with the corresponding destination address. When a connection request is made to this destination address, the request must go through the proxy server indicated. "(Do not use proxy)" means that a proxy server will not be used when connection requests are made to the corresponding destination address.
Proxy User ID	Specifies the user ID associated with a destination address and proxy server. User IDs can serve a variety of purposes: identification, definition of special privileges, etc. A user ID may or may not be required by the associated proxy server. Check with your system administrator to determine if a user ID is required.
New	Opens the **New Routing Filter** dialog box in which you can add new entries to the destination routing list
Delete	Deletes the selected entry on the destination routing list. You cannot delete the final entry in this list.
Change	Opens the **Change Routing Filter** dialog box in which you can edit the selected entry on the destination routing list. You cannot edit the destination in the final entry "Any address on any port".
	To bypass click the destination route for which you want to bypass the proxy server.
Up and Down arrows	Moves the selected entry up or down one line in the list.

Set up a SOCKS or HTTP Proxy Server Session

You can configure sessions to connect through a SOCKS proxy server or an HTTP server.

NOTE: SOCKS and HTTP are supported for VT, IBM 3270, and IBM 5250 terminals.

Before you start

Make sure your system has a proxy server or servers and that you know the following information:

- If you are setting up a connection to a SOCKS server, know the proxy server address and protocol version.
- If you are setting up a connection to an HTTP server, know the proxy server address and port.

To set up a session to connect through a SOCKS proxy server or an SSL/TLS server

1 Open the **Create New Document** dialog box.

 The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	From the Quick Access Toolbar, click the **New Document** ▯ button.
TouchUx	Tap the Folder icon and then under **File**, select ▯ **New**.

2 From the **Create New Document dialog** box, select a document template and click **Create**.

3 In the **Create New Terminal Document**dialog box, under **Connection**, enter the Host name/IP address.

4 Click **Configure additional settings** and then click **OK**.

5 In the Settings dialog box, under **Host Connection**, click **Setup Connection Security**.

6 If you are configuring a 3270 or 5250 terminal session, in the Configure Advanced Connection Settings dialog box, Under **Security**, click **Security Settings**.

7 On the Security Properties dialog box **Proxy**tab, select **Use proxy serve**r and then select whether to use the SOCKS or HTTP proxy type.

8 Click **Configure**.

9 If you want to designate only one HTTP proxy server, configure the session for the proxy server as follows:

To configure…	Do this
SOCKS	Enter the **Server address** and the **Protocol version**.
HTTP	Enter the server **Address** and **Port**.
	If you want to use authentication that requires a user name and password, select **Basic authentication** and enter the user name for the proxy server. (If this is not selected, no authentication is used.)

10 If you want to configure more than one proxy server or configure specific destination routes, leave the fields in the **HTTP** (or **SOCKS**) **proxy** group blank and click **Advanced**.

If you have trouble with HTTP timeouts, you can prevent them from occurring by configuring your proxy server so that it doesn't timeout. For IBM 3270 and IBM 5250 sessions, you can use another approach to keep sessions alive as shown below.

To keep sessions alive to prevent HTTP timeouts

1 In the Settings dialog box, under **Host Connection**, click **Setup Connection Security**.

2 In the Configure Advanced Connection Settings dialog box, Under **Keep Alive**, select **Keep Alive Packets**.

3 In the list under **Keep Alive**, select **Send Timing Mark Packets**.

4 Change the **Keep alive timeout in seconds** interval to a value that is less than the HTTP proxy timeout.

HTTP Configuration Dialog Box

Getting There

1 In the Security Properties dialog box, on the **Proxy** tab, click **Use proxy server**.

2 Under **Proxy type**, select **HTTP** and then click **Configure**.

Use this dialog box to designate HTTP proxy servers. You can designate a single HTTP proxy server through which all requested connections must pass or use **Advanced** options to designate multiple HTTP proxy servers.

HTTP proxy

Enter information to designate a single HTTP proxy server. If you want to configure more than one proxy server or configure specific destination routes, leave the fields in the **HTTP proxy** group blank and click **Advanced**.

Address	Enter the HTTP proxy server address.
Port	Enter the port of the proxy server.
Basic authentication	Select if you want to use authentication that requires a user name and password. (If this is not selected, no authentication is used.)
User ID	Enter the user name for the proxy server.
Advanced	Click to configure multiple HTTP proxy servers and destination routing filters for connection requests (see the following Advanced options).

Advanced options

Configure multiple proxy servers in order of preference. When a connection is requested, the client attempts to match the request with these addresses, beginning at the top of the list and moving down. The final line in the list, "Any address on any port", serves as a match for any request and prevents a connection request from being ignored.

To bypass a proxy server, select it from the list of destinations, click **Change**, and select the **Do not use...** check box.

Destination	Specifies the name or IP address as well as the port number of one or more destination hosts. (Asterisks in an IP address represent wildcard characters.)
Proxy	Specifies the name or IP address of the proxy server associated with the corresponding destination address. When a connection request is made to this destination address, the request must go through the proxy server indicated. "(Do not use proxy)" means that a proxy server will not be used when connection requests are made to the corresponding destination address.
Proxy User ID	Specifies the user ID associated with a destination address and proxy server. User IDs can serve a variety of purposes: identification, definition of special privileges, etc. A user ID may or may not be required by the associated proxy server. Check with your system administrator to determine if a user ID is required.
New	Opens the **New Routing Filter** dialog box in which you can add new entries to the destination routing list
Delete	Deletes the selected entry on the destination routing list. You cannot delete the final entry in this list.
Change	Opens the **Change Routing Filter** dialog box in which you can edit the selected entry on the destination routing list. You cannot edit the destination in the final entry "Any address on any port".
	To bypass click the destination route for which you want to bypass the proxy server.

| Up and Down arrows | Moves the selected entry up or down one line in the list. |

Routing Filter Dialog Box

Getting there

The way you access the **Security Properties** dialog box depends on the session type you are in.

Terminal session

1 Open the Document Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ⬚.
TouchUx	Tap the Gear icon and then select ⬚ **Document Settings**.

2 Under **Host Connection**, click **Setup Connection Security**.

3 (3270 and 5250 terminal sessions only) Under **Security**, click **Security Settings**.

Printer session

1 Open a printer session.

2 On the **Connection** menu, click **Session Setup**.

3 Click **Security**.

FTP Client

1 In the **Connect to FTP Site**dialog box, select a site.

2 Click **Security**.

Specify the destination routing filters for connection requests, for SOCKS or HTTP configurations.

NOTE: You cannot change the destination address and port of the final entry in the destination route list. You can, however, change the SOCKS or HTTP proxy information for this entry.

Destination address	Specifies the host name or IP address of the destination that is controlled by the associated proxy server (Asterisks in an IP address represent wildcard characters.)
Port	Specifies the port associated with the destination address.
Do not use SOCKS (or HTTP) proxy	When this check box is selected, a connection request matching this destination route will bypass the proxy server (destination).
SOCKS (HTTP) proxy	Specifies the **Address**, **Port**, and **User ID** of the proxy server. These settings are available only if **Do not use SOCKS (or HTTP) proxy** is cleared.

Security Properties Dialog Box

The Security Property dialog box is available from many Micro Focus products. The steps you use to open this dialog box depend on which product you are running.

The security options available to you in this dialog box depend on your product and session type.

In this Section

SSL/TLS (Security Properties Dialog Box)

The Secure Sockets Layer protocol (SSL) and its compatible successor, the Transport Layer Security protocol (TLS), enable a client and server to establish a secure, encrypted connection over a public network. When you connect using SSL/TLS, the client authenticates the server before making a connection, and all data passed between the client and the server is encrypted. Depending on the server configuration, the server may also authenticate the client.

The options are:

Use SSL/TLS Security	Enables SSL/TLS connections. You must select this before you can set other values on the SSL/TLS tab. When **Use SSL/TLS security** is selected, connections are made to the host only if a secure SSL/TLS connection can be established.
	Before making an SSL/TLS connection, your client must authenticate the host. Authentication is handled through the use of digital certificates. These certificates are part of the same Public Key Infrastructure (PKI) that is used to secure internet transactions. Your computer must be configured to recognize the digital certificate presented by your host and, if necessary, to provide a certificate for client authentication. If your computer is not properly configured, or if the certificates presented for authentication are not valid, you will not be able to make SSL/TLS connections. Depending on how a host certificate was issued, you may need to install a certificate on your local computer.
SSL/TLS version	Specifies which SSL or TLS version to use.

Encryption Strength	Specify the desired level of encryption for SSL/TLS connections. The connection will fail if this level cannot be provided.
	If you select **Recommended ciphers**, the FTP Client will negotiate with the host system to choose the strongest encryption level supported by both the host and the client. This new setting will contain the recommended encryption level from Micro Focus, and will change periodically.
	If you are running in FIPS mode and select **Recommended Ciphers**, the FTP Client will negotiate using only FIPS compliant encryption levels.
	If you select **Custom ciphers**, you will be prompted to select from a list of available ciphers in the **Custom Ciphers** list view.
	NOTE: Session files from previous versions of Reflection that use default, 168, 128 or 256 bit Encryption Strength will be imported as **Custom Ciphers** and maintain the list that was used in prior versions for those settings options.
Run in FIPS mode	When you run in FIPS mode, all connections are made using security protocols and algorithms that meet FIPS 140-2 standards. In this mode some standard connection options are not available. A FIPS mode icon is visible on the status bar when a connection is made using FIPS mode.
	NOTE: Selecting **Run in FIPS mode** on the **SSL/TLS** tab enforces FIPS mode only for the connection currently being configured. Administrators can use Group Policies to enforce FIPS mode for all connections.
Retrieve and validate certificate chain	Specifies whether certificates presented for host authentication are checked to determine if they are valid and signed by a trusted CA.
	CAUTION: Disabling this option can make connections vulnerable to man-in-the-middle attacks, which could compromise the security of the connection.
Use security proxy	Configure this session to use the Security Proxy for the server connection.
Implicit SSL/TLS Connection	IBM z/VM or z/OS Telnet servers can be configured to send the STARTTLS command when negotiating secure SSL/TLS connections. To connect to servers that are configured to send this command, unselect this option.
	To connect to servers that are not configured to send this command, leave this option selected. This option should be unselected for servers that require STARTTLS. When selected, secure connections to servers that send the STARTTLS command are not supported.

Security Proxy Server Settings

You can use settings under **Use security proxy** if you use a centralized management server (available separately from Micro Focus) to manage sessions and you launched this session from the Administrative WebStation. With these options, your session connects to your host via the Security Proxy included in the centralized management server. You can use this Security Proxy to configure secure connections even if your host is not running an SSL/TLS-enabled Telnet server. (Some of these settings are only visible when using the Administrative WebStation.)

NOTE

- When the Security Proxy is used, the connection between the client and the Security Proxy server is secured and encrypted using the SSL/TLS protocol. By default, the information sent between the proxy server and the destination host is in the clear. If you enable the **End-to-End encryption** option (available for 5250, 3270, and VT sessions), information sent between the Security Proxy the destination host is also encrypted. (**End-to-End encryption** requires that the host support SSL/TLS.)

- If you configure sessions that connect through the Security Proxy with authorization enabled, users must log on to the centralized management server before they can connect using these sessions.

Use security proxy	Configure this session to use the Security Proxy for the server connection.
Security proxy	Select the proxy server name from the drop-down list, which shows available servers.
Proxy port	Select the proxy server port from the drop-down list.
Destination host	If client authorization is enabled on the Security Proxy, enter the destination host name. If client authorization is not enabled, this box is read only.
	When you select a security port, the destination host configured to use that port is displayed automatically.
Destination port	If client authorization is enabled on the Security Proxy, enter the destination port. If client authorization is not enabled, this box is read only.
	When you select a security port, the destination port and destination host are displayed automatically.
End-to-End SSL/TLS (Client to proxy to destination host)	This option tunnels a direct SSL/TLS connection to the host, while still connecting through the Security Proxy Server. These connections require two certificates and two SSL/TLS handshakes—one for the client/proxy server connection and another for the client/host connection.
No data encryption from proxy to destination host	This option applies a null cipher to the direct SSL/TLS connection from the client to the host so that this connection is not encrypted. This does not affect the encryption of the SSL/TLS connection from the client to the proxy server that provides the "tunnel" for the client/host connection. When this option is selected, the data is encrypted from the client to the proxy server and unencrypted ("in the clear") from the proxy to the host.
Proxy cipher suites	A read-only list of cipher suites supported by this proxy host and port. This list is only visible when the product is launched from the Administrative WebStation (included with the centralized management server).

SSL/TLS (FTP Options)

These are available if you open the Security Properties dialog box from the FTP Client.

You will not see this tab if your Micro Focus product does not include the Reflection FTP Client.

The Secure Sockets Layer protocol (SSL) and its compatible successor, the Transport Layer Security protocol (TLS), enable a client and server to establish a secure, encrypted connection over a public network. When you connect using SSL/TLS, the client authenticates the server before making a connection, and all data passed between your client and the server is encrypted. Depending on the server configuration, the server may also authenticate the client.

The options are:

Use SSL/TLS Security	Enables SSL/TLS connections. You must select this before you can set other values on the SSL/TLS tab. When **Use SSL/TLS security** is selected, FTP Client will only connect to the host if a secure SSL/TLS connection can be established.
	Before making an SSL/TLS connection, FTP Client must authenticate the host. Authentication is handled through the use of digital certificates. These certificates are part of the same Public Key Infrastructure (PKI) that is used to secure internet transactions. Your computer must be configured to recognize the digital certificate presented by your host and, if necessary, to provide a certificate for client authentication. If your computer is not properly configured, or if the certificates presented for authentication are not valid, you will not be able to make SSL/TLS connections. Depending on how a host certificate was issued, you may need to install a certificate on your local computer.
SSL/TLS version	Specifies which SSL or TLS version to use.
Encryption Strength	Specify the desired level of encryption for SSL/TLS connections. The connection will fail if this level cannot be provided.
	If you select **Recommended ciphers**, the FTP Client will negotiate with the host system to choose the strongest encryption level supported by both the host and the client. This new setting will contain the recommended encryption level from Micro Focus, and will change periodically.
	If you are running in FIPS mode and select **Recommended Ciphers**, the FTP Client will negotiate using only FIPS compliant encryption levels.
	If you select **Custom ciphers**, you will be prompted to select from a list of available ciphers in the **Custom Ciphers** list view.
	NOTE: Session files from previous versions of Reflection that use default, 168, 128 or 256 bit Encryption Strength will be imported as **Custom Ciphers** and maintain the list that was used in prior versions for those settings options.
Run in FIPS mode	When you run in FIPS mode, all connections are made using security protocols and algorithms that meet FIPS 140-2 standards. In this mode some standard connection options are not available. A FIPS mode icon is visible on the status bar when a connection is made using FIPS mode.
	NOTE: Selecting **Run in FIPS mode** on the **SSL/TLS** tab enforces FIPS mode only for the connection currently being configured. Administrators can use Group Policies to enforce FIPS mode for all connections.

Encrypt Data Stream	Specifies whether or not data is encrypted when the FTP client is configured to use SSL/TLS encryption. When this checkbox is selected, all communication between your computer and the FTP server is encrypted. When this checkbox is cleared, the FTP command channel (which is used for all FTP commands, including your user name and password) is encrypted. However, the data channel (which is used for directory listings and the contents of the files you transfer) is not encrypted.
Clear command channel	When this is enabled, FTP Client sends a CCC command to the host. If the host supports this option, this turns off encryption for the command channel only.
Retrieve and validate certificate chain	Specifies whether certificates presented for host authentication are checked to determine if they are valid and signed by a trusted CA.
	CAUTION: Disabling this option can make connections vulnerable to man-in-the-middle attacks, which could compromise the security of the connection.
Use Reflection security poxy	Select this option to use a centralized management server (available separately from Micro Focus) to manage sessions launched from the Administrative WebStation.
Implicit SSL/TLS Connection	By default the FTP Client makes SSL/TLS connections using Explicit security. In order to establish the SSL connection, explicit security requires that the FTP client issue a specific command (AUTH TLS) to the FTP server after establishing a connection. If the server gives a success response, the client begins the TLS negotiation. The default FTP server port (21) is used.
	When you select **Implicit SSL/TLS Connection**, the FTP Client uses Implicit security. Implicit security automatically begins with an SSL connection as soon as the FTP client connects to the server; no AUTH TLS command is sent prior to the TLS negotiation.
	By default, the FTP Client uses port 990 for Implicit connections.
Connect through NAT server	Select this setting if your FTP Client connects through a NAT (Network Address Translation) server. When this setting is selected, the FTP Client ignores IP addresses in FTP commands returned from the server.

Security Proxy Server Settings

You can use settings under **Use security proxy** if you use a centralized management server (available separately from Micro Focus) to manage sessions and you launched this session from the Administrative WebStation. With these options, your session connects to your host via the Security Proxy included with the centralized management server. You can use this Security Proxy to configure secure connections even if your host is not running an SSL/TLS-enabled Telnet server. (Some of these settings are only visible when using the Administrative WebStation.)

NOTE

- When the Security Proxy is used, the connection between the client and the Security Proxy server is secured and encrypted using the SSL/TLS protocol. By default, the information sent between the proxy server and the destination host is in the clear. If you enable the

End-to-End encryption option (available for 5250, 3270, and VT sessions), information sent between the Security Proxy the destination host is also encrypted. (**End-to-End encryption** requires that the host support SSL/TLS.)

◆ If you configure sessions that connect through the Security Proxy with authorization enabled, users must log on to the centralized management server server before they can connect using these sessions.

Use Security proxy	Configure this session to use the Security Proxy for the server connection.
Proxy name	Select the proxy server name from the drop-down list shows, which shows available servers.
Proxy port	Select the proxy server port from the drop-down list.

PKI Configuration Dialog Box

The PKI Settings dialog box is available from many Micro Focus products. The steps you use to open this dialog box depend on which product you are running.

Use the **PKI Configuration** dialog box to configure PKI settings for SSL/TLS sessions.

NOTE: To configure PKI settings for Secure Shell sessions use the **PKI** tab in the **Reflection Secure Shell Settings** dialog box.

The options are:

Certificate host name must match host being contacted	Specifies whether host name matching is required when validating host certificates. When this is enabled (the default), the host name you configure for your session must exactly match a host name or IP address entered in either the **CommonName** or the **SubjectAltName** field of the certificate.
Use OCSP	Specifies whether your client session checks for certificate revocation using OCSP (Online Certificate Status Protocol) responders when validating host certificates. OCSP responders may be specified in the AIA extension of the certificate itself. You can also specify OCSP responders using the **OCSP** tab in the Reflection Certificate Manager.
Use CRL	Specifies whether your client session checks for certificate revocation using CRLs (Certificate Revocation Lists) when validating host certificates. CRLs may be specified in the CDP extension of the certificate itself. You can also specify CRL using the **LDAP** tab in the Reflection Certificate Manager.
	Note: The default value of this setting is based on your current system setting for CRL checking. To view and edit the system setting, launch Internet Explorer, and go to **Tools** > **Internet Options** > **Advanced.** Under **Security**, look for **Check for server certificate revocation**.

Client Authentication	Displays the options for selecting the client certificate.
	When **Automatically select client certificate** is selected, the first qualifying certificate is presented to the server.
	When **Prompt for certificate** is selected, all qualifying certificates are presented so you can select which certificate to use. If only one certificate qualifies, Reflection automatically uses that certificate.
	If you want to use a particular certificate, select **Use selected certificate for authentication** to open the Select Certificate dialog box and then select the certificate.
	NOTE: Reflection uses the Server Certificate Request message to determine whether certificates are qualified.
Reflection Certificate Manager	Opens the **Reflection Certificate Manager**.
View System Certificates	Opens the **Windows Certificate Manager**, which you can use to manage certificates in your system stores.

Secure Shell (Security Properties Dialog Box)

The **Secure Shell** section of the **Security Properties** dialog box is visible only if you are running the FTP Client.

You will not see this tab if your Micro Focus product does not include the Reflection FTP Client.

Secure Shell is a protocol for securely logging onto a remote computer and executing commands. It provides a secure alternative to Telnet, FTP, rlogin, or rsh. Secure Shell connections require both server and user authentication, and all communications pass between hosts over an encrypted communication channel. You can also use Secure Shell connections to forward X11 sessions or specified TCP/IP ports through the secure tunnel.

The options are:

Use Reflection Secure Shell	Specifies that the connection be made using the Secure Shell protocol. You must select this check box before you can set other items.
SSH Config scheme	Secure Shell settings are saved to the specified SSH configuration scheme and uses these settings whenever you specify this SSH configuration scheme name. If you leave this blank, the current host name is used for the SSH configuration scheme name.
Configure	Opens the **Reflection Secure Shell Settings** dialog box. Use this dialog box to configure additional Secure Shell settings.
SFTP	When this option is selected, the FTP Client will connect using SFTP (Secure FTP) protocol. SFTP supports fewer commands than the full FTP protocol.

Use structured listing data	This setting is relevant for Secure Shell servers. Use it as a troubleshooting tool if information from your server is missing or is not correctly displayed in the FTP Client's server pane. This setting specifies which data list style sent by the server is used to create the directory display in the right pane of the FTP Client. When this setting is not selected (the default), the FTP Client uses the standard UNIX-style data list. When it is selected, the FTP Client uses the structured data list.
Preserve timestamps and file attributes	This setting affects SFTP connections. When this option is selected, files transferred to and from the server retain their date, time, and file attributes.
	NOTE
	◆ If you have configured default file attributes for transfers from FTP Client using **Tools** > **Options** > **Attributes**, these values are applied even if this option is selected.
	◆ Server file dates are not preserved when files are dragged from the FTP Client to the Windows desktop or Windows explorer folder. Use the local pane of the FTP Client to preserve file dates.
Send Window Size	Changing Buffer size and Number of buffers can improve transfer speed. The optimum values depend on your network and server setup. Changing these values may also affect how quickly you can cancel a transfer.
Tunnel FTP using port forwarding	When this option is selected, data is forwarded from the port you specify for **Local port** through the SSH tunnel. With this configuration you have access to the full range of FTP commands. All communications are sent through the SSH tunnel. This includes FTP commands (including user name and password) and all transmitted data (including directory listings and the contents of the files you transfer).
Local port	Specifies the port used when Tunnel FTP using port forwarding is enabled.
FTP host is different than the Secure Shell host	When this setting is selected, all FTP communications are forwarded securely through the Secure Shell tunnel to the specified Secure Shell server, then in the clear from the Secure Shell server to the FTP server. Using this setting in combination with **SSH server address** and **SSH user name** is equivalent to using the following **ssh** command line:
| | ```
ssh -L FTP/<local port>:<FTP address>:21 <SSH user
name>@<SSH server address>
``` |
| **SSH server address** | This setting is available when **FTP host is different than the Secure Shell host** is enabled. Use it to specify the host running your Secure Shell server. |
| **SSH user name** | This setting is available when **FTP host is different than the Secure Shell host is enabled**. If the user login name is different on the Secure Shell and FTP servers, use this to specify the user name on the Secure Shell server.) |

Proxy (Security Properties Dialog Box)

You can configure your application to connect through a SOCKS or HTTP server.

NOTE: If you want to set up an SSH (Secure Shell) connection through a SOCKS or HTTP proxy server, use the Proxy tab in the **Reflection Secure Shell Settings** dialog to enable and configure the server, not the Proxy tab in the Security Properties dialog.

Use proxy server	Specifies to use a proxy server to make the connection. You must select this check box before you can set other items.
SOCKS proxy	Specifies to use a SOCKS proxy server.
HTTP proxy	Specifies to use an HTTP proxy server.
Configure	Opens the Configuration dialog box, in which you can enter the server address and other settings.

Firewall (Security Properties Dialog Box)

The **Firewall** tab of the **Security Properties** dialog box is visible only if you are running the FTP Client.

You will not see this tab if your Micro Focus product does not include the Reflection FTP Client.

Use Firewall	Enables connections through a firewall. You must select this check box before you can set other items.
Style	The FTP Client sends different commands for logging onto a firewall and connecting to an FTP server based on the server style you specify.
Server name	Specify the name of the firewall that you use to log onto an FTP server.
User name	Specify a valid user name registered on the firewall server. For case-sensitive servers, you must use the appropriate case.
	This setting is unavailable if **Style** is set to username@servername and the **Password authentication** check box is cleared.
Password authentication	This setting is available when **Style** is set to username@servername. If your firewall is set up to authenticate the user prior to opening a connection to an FTP server, select this check box.
	If you have selected a firewall style that requires authentication, this option is selected automatically and you cannot change it.
Save password	If the check box is selected, the string entered in the **Password** box is saved as obfuscated text in your FTP settings file. Each character in the password will display as an asterisk (*) in user interface text boxes and in the FTP command window.
	When this check box is cleared, the password is not saved, and you are prompted for a password each time an FTP server connection is opened using the firewall.

7 Printing

Reflection supports several types of printing. You can:

- Print the current IBM host screen or any web page.
- Configure Reflection for 3270 or 5250 printer emulation and use your local printer to print host print jobs.
- From a VT session, you can print the screen or the display memory.
- From a VT session, you can print lines as they appear on the screen, using the logging feature.

Printing from IBM Sessions

Reflection supports several types of printing. You can:

- Print the current host screen.
- Configure Reflection for 3270 printer emulation and use your local printer to print host print jobs.
- Configure Reflection for 5250 printer emulation and use your local printer to print host print jobs.

All three of these types of printing share some dialog boxes, such as **Page Setup** and **Print Setup**, but changes to shared dialog boxes in one session won't be saved in the same dialog box in a different session.

In this Section

3270 Printer Emulation

In this Section

Create a 3270 Printer Session

Reflection 3270 printer sessions emulate IBM 3287 printers. Data sent from the host to the printer session is passed on to the local printer.

To create a 3270 printer session from the Reflection Workspace

1 Open the Create New Document dialog box.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	From the Quick Access Toolbar, click the **New Document** 📄 button.
TouchUx	Tap the Folder icon and then under **File**, select 📄 **New**.

2 Select **3270 Printer** and click **Create**.

3 In the **Enter Host Name or IP Address** dialog box, type a host name or IP address, and click **Connect** to connect immediately, or **Cancel** to configure more than just the host name.

To create a 3270 printer session from the Windows Start menu

1 From the Windows Start menu, choose **All Programs** > **Micro Focus Reflection** > **Reflection IBM Printer**.

   Printer sessions created this way use 3270 printer emulation by default.

2 In the **Enter Host Name or IP Address** dialog box, type a host name or IP address, and click **Connect** to connect immediately, or **Cancel** to configure more than just the host name.

Related Topics

Associate a 3270 Printer Session with a Terminal Session

There are two ways to associate a 3270 terminal session with a printer session:

To	Link the terminal session to
Open the printer session automatically when the terminal session connects, and close it when the terminal session closes	A printer session document.
Retain manual control over opening and closing printer sessions	A printer session using an association string.

To link a terminal session to a printer session document

1   Open a 3270 terminal session.

2   Open the Document Settings dialog box.

    The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ![icon].
TouchUx	Tap the Gear icon and then select ![icon] **Document Settings**.

3   Under **Host Connection**, click **Configure Advanced Connection Settings**.

4   Under **TN3270 Enhanced Protocol**, select **Enable associated printer**.

5   Select the **Associated 3270 printer session** option.

6   Point to a 3270 printer session.

    Type the path and filename or click **Browse** to locate the file.

To link a terminal session to a printer session using an association string

1   Open a 3270 terminal session.

2   Open the Document Settings dialog box.

    The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ![icon].
TouchUx	Tap the Gear icon and then select ![icon] **Document Settings**.

3 Under **Host Connection**, click **Configure Advanced Connection Settings**.

4 Under **TN3270 Enhanced Protocol**, select **Enable associated printer**.

5 Select **Association string,** and type the association string you want to use.

6 Click **OK**.

7 Open a 3270 printer session.

Disconnect it if necessary. If you are creating a new session, don't connect to the host yet.

8 From the **Connection** menu, choose **Session Setup**.

9 Under Transport, from the **Connection type** list, choose **Associate**.

10 In the **TN Association** box, type the printer string you specified for **Association string** in your terminal session.

11 Click **OK**.

Related Topics

- "Create a 3270 Printer Session" on page 554
- "Configure Advanced Connection Settings Dialog Box" on page 299
- "Printing from IBM Sessions" on page 553

Session Setup Dialog Box (3270 Printer Sessions)

Getting there

1 Open a printer session.

2 From the **Connection** menu, choose **Session Setup**.

Use the **Session > Setup** dialog box to configure the connection to an IBM host for printer emulation sessions.

NOTE: You cannot configure the settings from this dialog box when you are connected to a host.

Session

Type	Select the type of printer session you want. The options on this dialog box (and the Help topic) change if you modify this setting.
Model ID	Reflection 3270 printer sessions emulate IBM 3287 printers.

Transport

Type	Select the transport to use.
Enter Host (or System) Name or IP Address	Identify the host to which you will connect. Type the host name, alias, or numeric IP address.
	NOTE: Both IPv4 addresses (in the form 127.0.0.1) and IPv6 addresses (in the form 2001:0db8:3c4d:0015:0000:0000:abcd:ef12) are accepted.

Port	Type the host port or socket number that the session should use. This field accepts any number between 0 and 66,535 (default = 23).
Connection type(Telnet Extended)	Select **Connect** when the LU name to which you are connecting is the name of a particular printer device. Select **Associate** to associate the printer session to a terminal session using an association string.
Host LU name	When you connect as a 3287 printer, some hosts require a host LU name. The name can be up to 32 characters in length.
TN association (Telnet Extended)	This option is available when **Connection type** is set to **Associate**. It displays a list of association strings you can configure using the **Configure Advanced Connection Settings** dialog box in a terminal session.
Advanced	Configure advanced Telnet settings.

Connect options

Auto connect	Select to establish a host connection as soon as the printer session is started.
Security	Secure data communications with SOCKS or SSL/TLS.

Related Topics

IBM 3270 Printer Panel

Reflection 3270 printer sessions emulate IBM 3287 printers. Data sent from the host to the printer session is passed on to the local printer.

The following items appear on the 3270 printer panel.

Printer Control

Hold/Enable	Click **Hold** to stop sending data to the printer. The word `Hold` appears in the **Status** box and the **Hold** button becomes the **Enable** button. While the printer is on hold, the **Reset** and **Flush**buttons become available. To cancel a hold, click **Enable**.
Cancel	Send a `Cancel Print` message to the host. `Cancelled` is displayed in the **Status** box.
Reset	Clear an error or cancel a condition. After a reset, printing continues (any hold is terminated and the status message becomes `Printing`.)
Flush	Force any pending printer output to the printer. If you're printing to a file, this action forces data to the file, and then closes the file.

Forms Control

Form feed	Advance the paper in the printer to the top of the next page. This button is available only when the printer is on hold.
Line feed	Advance the paper in the printer one line. This button is available only when the printer is on hold.

Host Control

PA1 and **PA2**	Send a Program Attention signal to the host.

Additional Items

Status	Displays printer status messages.
Test page	Print a test page. If you are connected, click **Hold** first. If no errors are detected, the printer goes back online automatically after the test.
Setup	Open the **Printer Session Setup** dialog box, from which you can configure host-related printing options.
Info	Display information about your current printer configuration and font selection.

Related Topics

Status Messages (3270 Printer Sessions)

Printer messages that appear in the **Status** box are color-coded:

◆ Green indicates that the printer session is online.

◆ Yellow indicates that the printer session is offline.

◆ Red indicates an error condition.

The messages that can appear in the **Status** box (and their respective colors) are:

Message	Meaning	Color
Bell	The Bell data stream control was received.	Green
Cancelled	The pending print job (if any) has been cancelled.	Yellow
Command Rejected	An invalid or unsupported data stream control was encountered.	Red
Data Check	Invalid print data was received.	Red
Disconnected	No host connection.	Yellow

Message	Meaning	Color
Error	An unknown error has occurred.	Red
Hold	The printer is offline.	Yellow
Host Link Down	The link between the gateway and the host has been lost.	Yellow
Operation Check	An illegal buffer address or incomplete data stream control was received.	Red
Printer Error	An error has occurred in writing to the printer.	Red
Printing	The printer is printing.	Green
Ready	The printer is ready to print.	Green

Related Topics

 ◆ "IBM 3270 Printer Panel" on page 557

 ◆ "Configure Printer Session Settings" on page 572

Advanced 3270 Telnet Dialog Box (Printer Sessions)

Getting there

1 Open a printer session.

2 From the **Connection** menu, choose **Session Setup**.

3 From the **Type** list, choose a printer session type.

4 Click the **Advanced** button.

The options are:

Terminal ID	This setting is not available when configuring Telnet Extended sessions.
	Specify a terminal model only if you are unable to connect to the host using the available Model ID settings from the Session Setup dialog box.
	If the host can't recognize the specified Telnet Terminal ID string, you may have difficulty connecting, or, once connected, you may experience emulation problems.
Telnet location	(Optional) Type up to 41 characters of descriptive text to provide information about your session. For example, you might include your PC's location, computer name, or IP address.
	This features uses the SEND-LOCATION option supported under Telnet connections (RFC779).
	Reflection does not initiate a WILL SEND command unless you activate the **Telnet location** option by typing information in this box.
Response mode(Telnet Extended)	Select to send a response from the PC each time a message is received from the host.
	For improved performance, clear this option.

Send Keep Alive packets	Select to provide a constant check between your session and the host so that you become aware of connection problems as they occur.

Choose one of the three types of keep-alive packets:

Choose	To cause
System	The TCP/IP stack to keep track of the host connection. This method requires less system resources than Send NOP Packets or Send Timing Mark Packets. However, most TCP/IP stacks send Keep Alive packets infrequently.
Send NOP Packets	Reflection to periodically send a No Operation (NOP) command to the host. The host is not required to respond to these commands, but the TCP/IP stack can detect if there was a problem delivering the packet.
Send Timing Mark Packets	Reflection to periodically send a Timing Mark Command to the host to determine if the connection is still active. The host should respond to these commands. If Reflection does not receive a response or there is an error sending the packet, it shuts down the connection.

Keep Alive timeout in seconds	Select the interval between the keep-alive requests. The range of values is 1 to 9999 seconds; the default value is 600 seconds.

Printer Session Setup Dialog Box (3270 Printer Sessions)

Getting there

1 Open a 3270 printer session.
2 From the printer panel, click the **Setup** button.

The options are:

Character translation

National character set	Determines how host characters (EBCDIC) are mapped to PC characters (ANSI). This setting should match the national character set used by your host system.
Country Extended Graphics Code	Select to make additional characters available in the configured **National character set**. See your host documentation for details.
Transparent mode	Select this check box for printer-ready documents that require no page formatting. In **Transparent mode**, all page format settings (**Characters per line** and **Lines per page**) are ignored.
Translate EBCDIC in SCS TRN transparent mode	When this check box is selected, Reflection translates EBCDIC characters in the SCS TRN command.
Bypass Windows print driver in transparent mode	Select to disable Windows handling of fonts, font size, font style, and lines-per-inch configuration while in **Transparent** mode.

Flush printing options

Flush when End of Job record received	Select if you want an in-progress print job to close if an end-of-job condition is sent from the host.
Host print timeout for flushing	Specify the number of seconds to wait after the host stops sending data to a printer session before forcing all pending printer output to the printer.

Form feed options

Emulate form feed with line feed	Select to have Reflection simulate a form feed by issuing line feeds until the end of the page is reached.
Send form feed at end of job	Select to send a form feed at the conclusion of host print jobs.

Related Topics

5250 Printer Emulation

In this Section

Create a 5250 Printer Session

Reflection 5250 printer sessions emulate IBM 3812 printers. Data sent from the host to the printer session is passed on to the local printer.

To create a 5250 printer session from the Reflection Workspace

1 Open the Create New Document dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	From the Quick Access Toolbar, click the **New Document** button.
TouchUx	Tap the Folder icon and then under **File**, select New.

2 Select **5250 Printer** and click **Create**.

3 In the **Enter Host Name or IP Address** dialog box, type a host name or IP address, and click **Connect** to connect immediately, or **Cancel** to configure more than just the host name.

To create a 5250 printer session from the Windows Start menu

1 From the Windows Start menu, choose **All Programs** > **Micro Focus Reflection** > **Reflection IBM Printer**.

Printer sessions created this way use 3270 printer emulation by default.

Use the following steps to change to a 5250 printer session.

2 Click **Cancel** to close the **Enter Host Name or IP Address** dialog box.

3 From the **Connection** menu, choose **Session Setup**.

4 Under **Session**, from the **Type** list, choose IBM 5250 Printer.

5 For **Host Name/IP Address**, enter the fully qualified host name.

6 Click **Connect** to connect immediately, or click **OK** to configure additional settings.

Related Topics

- "Configure Printer Session Settings" on page 572
- "IBM 5250 Printer Panel" on page 564
- "Printing from IBM Sessions" on page 553

Session Setup Dialog Box (5250 Printer Sessions)

Getting there

1 Open a printer session.

2 From the **Connection** menu, choose **Session Setup**.

Use the **Session > Setup** dialog box to configure the connection to an IBM host for printer emulation sessions.

Note: You cannot configure the settings from this dialog box when you are connected to a host.

Session

Type	Select the type of printer session you want. The options on this dialog box (and the Help topic) change if you modify this setting.
Model ID	Select the printer model to emulate.

Transport

Type	5250 printer sessions use Telnet.
Enter Host (or System) Name or IP Address	Identify the host to which you will connect. Type the host name, alias, or numeric IP address.
	NOTE: Both IPv4 addresses (in the form 127.0.0.1) and IPv6 addresses (in the form 2001:0db8:3c4d:0015:0000:0000:abcd:ef12) are accepted.
Port	Type the host port or socket number that the session should use. This field accepts any number between 0 and 66,535 (default = 23).
Device name	Specify the terminal device name (also called the display name or the workstation ID) that the IBM System i should use for your session. If you leave this box blank, the IBM System i creates a device to use for your session.
	The device name can be up to ten characters long. You can include any of the following characters as part of the value in the **Device name** box.

Character	Usage
*	Replaced by A, B, C, and so on to create a unique device name. If the entire alphabet is used, the generated device names continue with AA, AB, AC, and so on.
%	Replaced by P for printer sessions and S for display sessions.
=	Replaced by 1,2, 3, and so on to create a unique device name.
&COMPN	Replaced by the local workstation name, left-trimmed, if the generated name exceeds 10 characters.
&USERN	Replaced by the local user name, left-trimmed, if the generated name exceeds 10 characters.
+	Specifies right-trimming instead of left-trimming. Use with &COMPN or &USERN. This character can be placed anywhere in the string.

NOTE

- ◆ You can use only one string in combination with these characters. If you use separated strings, the second string is dropped. For example, %MyDevice= is valid. However, %My=Device is not valid, and will be treated by the system as if it were &My=.

- ◆ You cannot use both &COMPN and &USERN in the same string.

- ◆ To have Reflection generate unique device names automatically based on the special characters described above, the **Generate Device Names** setting must be enabled. In printer sessions, this setting is off by default.

Advanced	Configure advanced Telnet settings.

Connect options

Auto connect	Select to establish a host connection as soon as the printer session is started.
Initialize	Create and initialize printer devices on your IBM System i host.
Security	Secure data communications with SOCKS or SSL/TLS.

Related Topics

IBM 5250 Printer Panel

Reflection 5250 printer sessions emulate IBM 3812 printers. Data sent from the host to the printer session is passed on to the local printer.

The following items appear on the 5250 printer panel.

Printer Control

Hold/Enable	Click **Hold** to stop sending data to the printer. The word `Hold` appears in the **Status** box and the **Hold** button becomes the **Enable** button. While the printer is on hold, the **Reset** and **Flush**buttons become available. To cancel a hold, click **Enable**.
Cancel	Send a `Cancel Print` message to the host.
	`Cancelled` is displayed in the **Status** box.
Reset	Clear an error or cancel a condition.
	After a reset, printing continues (any hold is terminated and the status message becomes `Printing`.)
Flush	Force any pending printer output to the printer. If you're printing to a file, this action forces data to the file, and then closes the file.

Forms Control

Form feed	Advance the paper in the printer to the top of the next page. This button is available only when the printer is on hold.
Line feed	Advance the paper in the printer one line. This button is available only when the printer is on hold.

Additional Items

Status	Displays printer status messages.
Test page	Print a test page. If you are connected, click **Hold** first. If no errors are detected, the printer goes back online automatically after the test.
Setup	Open the **Printer Session Setup** dialog box, from which you can configure host-related printing options.
Info	Display information about your current printer configuration and font selection.

Related Topics

Status Messages (5250 Printer Sessions)

Printer messages that appear in the **Status** box are color-coded:

- Green indicates that the printer session is online.
- Yellow indicates that the printer session is offline.
- Red indicates an error condition.

The messages that can appear in the **Status** box (and their respective colors) are:

Message	Meaning	Color
Bell	The Bell data stream control was received.	Green
Cancelled	The pending print job (if any) has been cancelled.	Yellow
Connected	Indicates the session is connected, but the host is not yet ready to send print data.	Yellow
Disconnected	No host connection.	Yellow
Error	An unknown error has occurred.	Red
Exception *nn*	A data stream formatting error has been encountered; nn is the exception code.	Red
Hold	The printer is offline.	Yellow

Message	Meaning	Color
Host Link Down	The link between the gateway and the host has been lost.	Yellow
Printer Error	An error has occurred in writing to the printer.	Red
Printing	The printer is printing.	Green
Ready	The printer is ready to print.	Green

Related Topics

- "Exception Messages (5250 Printing)" on page 566
- "Configure Printer Session Settings" on page 572

Exception Messages (5250 Printing)

If you are running a 5250 printer emulation code, you may see an exception code display in the printer panel **Status** box. Refer to the following table for more information.

Code	Meaning
10	The data stream control is unsupported or unrecognized.
11	Printing will occur outside the specified left or right margin.
12	An illegal superscript or subscript character was received.
13	The data stream control is not supported unless the **Bypass Windows print driver in transparent mode** (page 569) check box is selected.
14	A graphics character is unprintable.
15	The data stream control is not supported while the **Bypass Windows print driver in transparent mode** (page 569) check box is selected.
16	Printing will occur above or below the specified top or bottom margin.
17	A control in the data stream is illegally nested.
20	A supported control exists at an invalid position in the data stream.
21	An invalid indent level was received or there is no tab stop at the specified indent level.
22	No horizontal tab stop setting found.
23	The length of a line exceeds the justified right margin or the margin exceeds the page width.
24	Backspacing will occur beyond the leftmost physical print position.
25	Text will be printed below the bottom of the page.
26	Justify control violation.
30	Unsupported data stream control.
31	A required control parameter is missing.
32	An unsupported control parameter has been detected.

Code	Meaning
40	Invalid parameter value in multi-byte control.

Related Topics

- "Status Messages (5250 Printer Sessions)" on page 565
- "Printer Session Setup Dialog Box (5250 Printer Sessions)" on page 569
- "IBM 5250 Printer Panel" on page 564

Advanced 5250 Telnet Dialog Box (Printer Sessions)

Getting there

1 Open a printer session.

2 From the **Connection** menu, choose **Session Setup**.

3 From the **Type** list, choose a printer session type.

4 Click the **Advanced** button.

The options are:

Telnet location	(Optional) Type up to 41 characters of descriptive text to provide information about your session. For example, you might include your PC's location, computer name, or IP address.
	This features uses the SEND-LOCATION option supported under Telnet connections (RFC779).
	Reflection does not initiate a WILL SEND command unless you activate the **Telnet location** option by typing information in this box.
Send Keep Alive packets	Select to provide a constant check between your session and the host so that you become aware of connection problems as they occur.
	Choose one of the three types of keep-alive packets:

Choose	To cause
System	The TCP/IP stack to keep track of the host connection. This method requires less system resources than Send NOP Packets or Send Timing Mark Packets. However, most TCP/IP stacks send Keep Alive packets infrequently.
Send NOP Packets	Reflection to periodically send a No Operation (NOP) command to the host. The host is not required to respond to these commands, but the TCP/IP stack can detect if there was a problem delivering the packet.

Send Timing Mark Packets	Reflection to periodically send a Timing Mark Command to the host to determine if the connection is still active. The host should respond to these commands. If Reflection does not receive a response or there is an error sending the packet, it shuts down the connection.
Keep Alive timeout in seconds	Select the interval between the keep-alive requests. The range of values is 1 to 9999 seconds; the default value is 600 seconds.

Related Topics

5250 Printer Device Initialization Dialog Box

Getting there

1 Open a 5250 printer session.

2 From the **Connection** menu, choose **Session Setup**.

3 Click the **Initialize** button.

Create and initialize 3812 printer devices on your IBM System i host.

The options are:

Message library	Select the library that contains the message queue for exception messages. Consult your system administrator before changing this value.
Message queue	Select the message queue to which exception messages should be sent. For example, the IBM System i may need to tell the printer to switch to another paper tray. Consult your system administrator before changing this value.
Font typestyle ID	Select the default font typestyle to use for printing.
Forms mode	Select the way forms are fed into the printer.

Select	To feed
*AUTOCUT	Single-cut sheets into the printer automatically.
*CONT	Continuous forms into the printer automatically.
*CUT	Single-cut sheets into the printer manually.

Host Print Transform

Host print transform	Select to specify the manufacturer type and model, the paper sources, and the envelope source on your IBM System i print device.

Manufacturer type	Select a printer manufacturer type and model. This must match a manufacturer type and model string defined on the IBM System i. If your printer does not appear in the list, ask your system administrator for the string identifying your printer, and type it in.
	If you select a printer that begins with *WSCST, you must also specify the **Workstation Customizing Object > Name** and **Library**, which the IBM System i will use to print jobs.
Paper source 1	Select the primary paper source on the host printer. You can specify a particular paper size or one of the following:

Select	To do this
*MFRTYPMODEL	Substitute the value most common for your printer.
*NONE	No paper source is specified.
*SAME	Use the currently configured host value.
Windows Printer	Use the value specified by the default Windows printer.

Paper source 2	Select the secondary paper source on the host printer.
Envelope source	Select the envelope source on the host printer.
Name	Type the name of a workstation customizing (WSCST) object that gives the IBM System i information about the functions supported by your ASCII printer.
Library	Select the location of the WSCST object.

Related Topics

- "Configure Printer Session Settings" on page 572
- "Session Setup Dialog Box (5250 Printer Sessions)" on page 562

Printer Session Setup Dialog Box (5250 Printer Sessions)

Getting there

1 Open a 5250 printer session.

2 From the printer panel, click the **Setup** button.

The options are:

Character translation

National character set	Determines how host characters (EBCDIC) are mapped to PC characters (ANSI). This setting should match the national character set used by your host system.
Transparent mode	Select this check box for printer-ready documents that require no page formatting. In **Transparent mode**, all page format settings (**Characters per line** and **Lines per page**) are ignored.
Bypass Windows print driver in transparent mode	Select to disable Windows handling of fonts, font size, font style, and lines-per-inch configuration while in **Transparent** mode.

Flush printing options

Flush when End of Job record received	Select if you want an in-progress print job to close if an end-of-job condition is sent from the host.
Host print timeout for flushing	Specify the number of seconds to wait after the host stops sending data to a printer session before forcing all pending printer output to the printer.

Form feed options

Emulate form feed with line feed	Select to have Reflection simulate a form feed by issuing line feeds until the end of the page is reached.
Send form feed at end of job	Select to send a form feed at the conclusion of host print jobs.
Font mapping (button)	Click to open the **Fonts** dialog box, from which you can map your local printer fonts to typestyle IDs used by a host.

Related Topics

- "Configure Printer Session Settings" on page 572
- "Session Setup Dialog Box (5250 Printer Sessions)" on page 562
- "Font Mapping (5250 Printer Sessions)" on page 570
- "Fonts Dialog Box" on page 571

Font Mapping (5250 Printer Sessions)

You can map local printer fonts to typestyle IDs used in IBM System i documents. You can then insert these typestyle IDs into source documents on the IBM System i, and assign various font, style, and size configurations to these typestyle IDs.

If you don't map typestyle IDs to fonts, Reflection attempts to match the font. However, the output may only approximate what is specified in the documents.

To map a typestyle ID to a font

1 Open a 5250 printer session.

2 From the printer panel, click the **Setup** button.

3 From the **Printer Session Setup** dialog box, click the **Font mapping** button.

4 From the **Fonts** dialog box, type a number in the **Typestyle ID** text box.

5 Select a font, font size, and font style.

6 Click **Map font to ID**.

A line similar to the following is added to the **Mapped fonts** box:

```
151    Courier,           10,  Regular
```

In this case, the display shows that text associated with typestyle ID 151 will be printed in 10-point Courier, in a regular style (that is, neither bold nor italic).

Related Topics

- "Fonts Dialog Box" on page 571
- "Printer Session Setup Dialog Box (5250 Printer Sessions)" on page 569
- "Configure Printer Session Settings" on page 572

Fonts Dialog Box

Getting there

1 Open a 5250 printer session.

2 From the printer panel, click the **Setup** button.

3 From the **Printer Session Setup** dialog box, click the **Font mapping** button.

The options are:

Typestyle ID	Select a typestyle ID used in your IBM System i documents to map to a local Windows font.
Font	Select a local Windows font to map to the selected typestyle ID.
Size	Select a size to map to.
Font style	Select a style to map to. The styles available depend on the font selected.
Sample	A sample of the local Windows font is displayed when a font, size, and style have all been specified.
Script	Select a language script to make the character set for that language available. The scripts available depend on the font selected.
Mapped fonts	This list displays all of the fonts you have mapped for the current session.
Map font to ID	With a typestyle ID selected, and a local Windows font, size, and style selected, click this button to map the font to the ID.
Clear font mapping	To delete a mapping, select an item from the Mapped fonts list, and then click this button.

Related Topics

- "Font Mapping (5250 Printer Sessions)" on page 570
- "Printer Session Setup Dialog Box (5250 Printer Sessions)" on page 569

Configure Printer Session Settings

Using Reflection printer sessions, you can print host jobs using your Windows printer.

To configure printer session settings

1 Open a printer session.

2 Configure settings using any of the following:

To	From the printer panel, do this
Configure the connection to an IBM host	From the **Connection** menu, choose **Session Setup**. The **Session Setup** dialog box appears.
Configure host-related printing options	Click **Setup**. The **Printer Session Setup** dialog box appears.
Configure the way text and images are arranged on the page	From the **File** menu, choose **Page Setup**.
Select a printer or configure printer properties	From the **File** menu, choose **Print Setup**.
View a complete list of current printing settings	From the **Setup** menu, choose **View Settings**.

3 To save the changes to your printer session file, from the printer panel, from the **File** menu, choose **Save**.

Printer session files use a *.rsf file extension.

Related Topics

- "Create a 3270 Printer Session" on page 554
- "IBM 3270 Printer Panel" on page 557
- "Create a 5250 Printer Session" on page 561
- "IBM 5250 Printer Panel" on page 564
- "Reset Printer Session to Defaults" on page 579

Enter Host (or System) Name or IP Address Dialog Box

This dialog box appears when you start a session for which no host has been specified. (This is the default configuration for a new printer session).

The options are:

Enter Host (or System) Name or IP Address	Type the host name or IP address of the terminal to which you want to connect.
Connect	Click to connect the session immediately.
Cancel	Click to configure more than just the host name for this session.

> ◆ If you are setting up a printer session, configure the session in the IBM 3270 (or 5250) Printer dialog box.
>
> ◆ If you are setting up a host session, on the quick access toolbar at the top of the workspace, click ⬚. Then, under **Host Connection**, click **Configure Connection Settings**.

Related Topics

- "Configure Printer Session Settings" on page 572
- "Create a 3270 Printer Session" on page 554
- "Session Setup Dialog Box (3270 Printer Sessions)" on page 556
- "Create a 5250 Printer Session" on page 561
- "Session Setup Dialog Box (5250 Printer Sessions)" on page 562
- "Connect and Save your Connection Settings" on page 22
- "Specify Whether to Automatically Connect to the Host" on page 56

Choose Template Dialog Box

Getting there

1 Open a printer session.

2 From the **File** menu, click **New Session**.

The options are:

Current settings	Create a new printer session using the same settings as your current session.
Default 3270 Printer	Create a new 3270 printer session.
Default 5250 Printer	Create a new 5250 printer session.

Related Topics

- "Configure Printer Session Settings" on page 572

Page Setup Dialog Box

Getting there (host screen printing)

1 Open a terminal session.

2 Open the Page Setup dialog box as follows:

The steps depend on your user interface mode (page 216).

- If you are using the Ribbon or Browser mode, click on the Quick Access Toolbar and then click **Page Setup**.

- If you are using the TouchUx mode, tap the Folder icon and then under **Print**, select **Page Setup**

Getting there (printer emulation)

1 Open a printer session.

2 From the **File** menu, choose **Page Setup**.

Configure page layout options for host screen printing and printer emulation sessions.

Paper

Size	Select the size of the paper or envelope you want to use.
Source	Choose the tray where the paper you want to use is located in the printer. Different printer models support different paper sources.

Orientation

Choose how the document is positioned on the page. The Page Preview at the top of the dialog box shows an example of the currently selected orientation.

Margins (inches)

Use the settings in this group box to set the printing area for the page. Reflection will not print outside the boundaries you specify. The Page Preview at the top of the dialog box shows an example of the currently selected margins.

Override the orientation specified by the host	Select to make sure that your selected orientation is used.
	In terminal sessions, page orientation is not set explicitly by the host but may be implied by the host page size. For example, by default the host page size is defined by the number of columns and lines on the terminal display. If the display is narrower than it is long, portrait orientation is implied. If the display is wider than it is long, landscape orientation is implied.
	In printer sessions, the host may explicitly set a particular orientation in the data stream, or an orientation may be implied by the host page size, as described above for terminal sessions.
Page Options	Open the **Page Options** dialog box, from which you can set the font to use for printed output, and specify the number of rows and columns to appear on the page.

Related Topics

- "Page Options Dialog Box" on page 575
- "Configure Printer Session Settings" on page 572
- "Printing IBM Host Terminal Screens" on page 581
- "Printing from IBM Sessions" on page 553

Page Options Dialog Box

Getting there

1 Open a terminal session.

2 Open the Page Setup dialog box as follows:

The steps depend on your user interface mode (page 216).

- If you are using the Ribbon mode, on the **File** menu, mouse over **Print**, and then choose **Page Setup**.
- If you are using the Classic mode, from the **File** menu, choose **Page Setup**.

3 From the **Page Setup** dialog box, click the **Page Options** button.

Configure text layout options for host screen printing and printer emulation sessions.

Text Format

Use printer fonts only	Select to print using only fonts residing on the host printer.
Override host page format	When this check box is selected, page formatting specified in the printer session document (**Characters per line**, **Lines per page**, **Font**, and **Margins**) is used regardless of what the host specifies.
Font	Select a font to use.
	NOTE: When you print all or part of a host screen from a terminal session, the font used is the currently configured display font, not the printer font setting configured here.
Page Scaling	Click to open the **Page Scaling** dialog box.

Characters per line

Select the maximum number of characters that can be printed on a single line. If a line longer than this value is sent from the host, the line is automatically wrapped.

These settings are ignored when, from the **Printer Session Setup** dialog box, **Transparent mode** is selected.

Lines per page

Select the number of lines to be printed on each page.

These settings are ignored when, from the **Printer Session Setup** dialog box, **Transparent mode** is selected.

Related Topics

- "Page Setup Dialog Box" on page 574
- "Configure Printer Session Settings" on page 572
- "Printing IBM Host Terminal Screens" on page 581
- "Printing from IBM Sessions" on page 553

Page Scaling Dialog Box

Getting there

1 Open a printer session.

2 Open the Page Setup dialog box as follows:

The steps depend on your user interface mode (page 216).

- If you are using the Ribbon mode, on the **File** menu, mouse over **Print**, and then choose **Page Setup**.
- If you are using the Classic mode, from the **File** menu, choose **Page Setup**.

3 Select Page Options.

4 From the **Page Options** dialog box, click the **Page Scaling** button.

The options are:

Scaling Options

No scaling	When you select **No Scaling**, Reflection prints the screen or host print job as it is received from the host.
Scale the page size specified by the host to fit on the Windows printer page	Automatically reduce or expand the page size specified by the host to fit the page size currently defined in the **Page Setup** dialog box.
Choose a host page size and scale it to fit on the Windows printer page	When selected, enables the **Host page size** list box.
	If you can get better results scaling from a host page size that is different from the one specified by the host, you can select one from the **Host page size** list.
Host page size	Select the size that best matches the form printout defined on the host.
Use scaling factors for reduction or expansion	Reduce or enlarge the width and length of the host print job and print it on the page size currently defined in the **Page Setup** dialog box.

NOTE

 ◆ No scaling is performed if either **Print to file** or **Bypass Windows print driver** is selected in the **Print Setup** dialog box.

 ◆ If the host does not explicitly set a particular page orientation, one may be implied by the host page size. If the host page is narrower than it is tall, portrait orientation is implied. If the host page is wider than it is tall, landscape orientation is implied. To make sure that the Windows printer orientation is used, from the **Page Setup** dialog box, select **Override the orientation specified by the host**.

Related Topics

Print Setup Dialog Box

Getting there (host screen printing)

1 Open a terminal session.

2 Open the Print dialog box as follows:

  ◆ If you are using The Ribbon mode, click ⎙ on the Quick Access Toolbar and then click **Setup**.

  ◆ If you are using the Classic mode, from the **File** menu, choose **Print Settings**

Getting there (printer emulation)

1 Open a printer session.

2 From the **File** menu, choose **Print Setup**.

The options are:

Printer

Name	Select a printer from this list of printers currently connected to your computer.
Properties	Click to set printer-specific options.
Status, Type, Where, Comment	These read-only fields describe the selected printer.

Print to file

Print to file	Select to send output to a file instead of a printer.
Print output to	Type the path and filename for the output file.
If file exists	Select what to do when the output file already exists in the target location.
Bypass Windows print driver	Select to send raw data (including printer control escape codes) directly to your printer. Output is sent to the printer immediately, instead of waiting for a whole page of information, and the Windows printing interface is bypassed.
	If you're bypassing Windows printing to a PostScript printer, the results may not be what you expect. PostScript printers are controlled by PostScript commands, which are typically sent to the printer from a PostScript printer driver.
Network	Click to connect to a shared network printer.
Types	Select to open the Print Types dialog box, where you can select a custom template that is set up to format data so it can be printed to a form. To select the template for the form you want to print, select **RTF Template Merge** in the **Print Types** list and browse to the template. (The default **Normal** print type prints the data in a standard format.)

Schemes	Select to open the Print Schemes dialog box where you can save the name of the printer and custom merge template you have selected in a print scheme file or load a print scheme that you have previously saved.

Multiple screens per page

Auto formfeed	Select to add a form feed between each screen print.
Close printer manually	Select to send multiple screen prints to a spool file and then print them all at once. (The spool file is sent to the printer when you click the **Close Printer** button on the status bar.)

Related Topics

- "Configure Printer Session Settings" on page 572
- "Printing IBM Host Terminal Screens" on page 581
- "Page Setup Dialog Box" on page 574
- "Print More Than One Screen per Page" on page 121

Printing to a Form or Label

For information about configuring Reflection to print to a form or label, refer to Technical Note 7021494 (https://support.microfocus.com/kb/doc.php?id=7021494).

This technical note details techniques that can be used to configure a print job to fit onto a pre-printed form, such as an invoice or tax document, where the output must align with specifically located fields.

Related Topics

- "Configure Printer Session Settings" on page 572

Reset Printer Session to Defaults

You can create a new session using the templates provided, or use the following procedure to return the settings of your current procedure to the defaults.

To reset default printer values for the current session

- From the **Setup** menu, select **Defaults**.

NOTE

- The **Defaults** command is not available when you are connected to a host.
- This action has no effect on saved settings files.

Related Topics

- "Choose Template Dialog Box" on page 573

Run a Trace (Printer Sessions)

If you are troubleshooting problems with a printer session, technical support may request that you obtain one or more traces.

To create a trace file for a printer session

1 Open a printer session.

  If you are connected to the host, disconnect (**Connection** > **Disconnect**).

2 From the **Connection** menu, chose **Trace** > **Start Trace**.

3 Select the trace file type.

Trace File Type	Description
Host-data trace (*.hst)	Captures information passed between a terminal or printer session and the host. This type of trace is useful when a host connection is working, but the terminal or printer session does not behave as expected.
	Host traces are not useful when a connection to the host cannot be established.
Command trace (*.cmd)	Captures actions within Reflection. Each action, such as clicking a button or entering text, represents an individual command. Command traces are useful in determining whether commands are correct in a script, macro, or program using OLE automation. Command traces can also be used to determine which command to use when writing a script.
	Use a text editor to view the command trace, and to determine which commands are needed to accomplish the task.

4 Specify a name for the trace file.

NOTE: If you have spoken with a support technician, use your call ID number as the name of your trace file.

---

5 Click **Trace**.

  A bug symbol appears in the status bar, indicating that the trace is active.

6 Connect to the host.

7 Perform the actions that reproduce the problem you want recorded in the trace.

8 To end the trace, go to **Connection** > **Trace** > **Stop Trace**.

Upload the trace file as a binary file to http://upload.attachmate.com (http://upload.attachmate.com). If the problem relates to a service request you are currently working on with a technician, include the Micro Focus service request number with the trace and let the technician know when the file is uploaded.

Related Topics

Save Changes on Exit (Printer Sessions)

By default, you see the **Save Changes on Exit** dialog box if you have made any changes to settings in the current session.

NOTE: To change the default behavior, edit the **Save Changes on Exit** setting in the **View Settings** dialog box.

The options are:

View Changes	Displays the **View Settings** dialog box, which shows settings which have been changed from the defaults.
Save	Exits and saves the changes .
Discard	Exits without saving the changes.
Cancel	Cancels the exit command and returns you to the session without saving the changes.

Printing IBM Host Terminal Screens

In this Section

Print a Terminal Screen

You can print the contents of the current terminal screen display.

To print a terminal screen using default print settings

1 Open a terminal session.

2 Navigate to the screen you want to print.

3 Open the Print dialog box.

The steps depend on your .

- If you are using the Ribbon or Browser mode, click ⊟ on the Quick Access Toolbar. Then, in the Print dialog box, click **Setup**.
- If you are using Classic mode, from the File menu, choose **Print Settings** or **Print Setup**

4 In the Print dialog box, click **OK**.

To modify the screen print settings

1 Open a terminal session.

2 Navigate to the screen you want to print.

3 Open the Print dialog box.

The steps depend on your .

- If you are using the Ribbon or Browser mode, click ⊟ on the Quick Access Toolbar. Then, in the Print dialog box, click **Setup**.
- If you are using Classic mode, from the File menu, choose **Print Settings** or **Print Setup**

4 From the **Print** dialog box, modify the desired settings.

5 Click **OK**.

Related Topics

- "Integrate Host Data with Office Tools" on page 69
- "Print Dialog Box (Terminal Screen Printing)" on page 582

Print Dialog Box (Terminal Screen Printing)

Getting there

1 Open a terminal session.

2 Open the Print dialog box as follows:

- If you are using Ribbon or Browser mode, click ⊟ on the Quick Access Toolbar.
- If you are using TouchUx mode, tap the Folder icon and then under **Print**, select **Print**

Options

Copies	Select the number of copies you want to print.
Fast text-only printing	Print using the current printer font, rather than the display font, and use white for the background.
Print status line	Select to print the host status line in addition to the terminal screen.
Monochrome	Select to print the screen using black and white only. To print the display in color or to print it using grayscale on a non-color printer, clear this check box.
Square aspect ratio	(3270 sessions only) Select to use the pixel dimensions of the 3179-G terminal, and ensure that objects maintain their correct proportions and shapes.
Background	Select a background color.

Print Range

All	Print the complete contents of the terminal window, including the host status line.
Selection	Print the currently highlighted selection.
Partition	(3270 sessions only) Print the current screen partition (which usually corresponds to the entire terminal window, but without the Operator Information Area).
Setup	Click to control printer settings that apply only to Reflection, or to select a different Windows printer.
Print what	(3270 graphics sessions only) Select the part of the terminal display to print: graphics, text, or both.
Document title	(Available only when **Fast text-only printing** is selected.)
	Enter the document title. (This text will be inserted where `&F` appears in the document header or footer text.)

Header text	(Available only when **Fast text-only printing** is selected.)
	Enter text or any of the following special characters in the header.

- `&D` inserts the current date in the format month-day-year (for English) or in an appropriate format for the current locale.
- `&T` inserts the current time in International format (for example, 14:29:22.86).
- `&F` inserts the document title or, if no title is specified, the session document name.
- `&P` inserts the page number.
- `&U` inserts the configured IBM System i sign-on user ID. If there is no IBM System i sign-on user ID, the current Windows user ID is inserted.
- `&H` inserts the configured host name.
- `&N` inserts a new line.
- `&&` inserts an ampersand ('&').

Footer text	(Available only when **Fast text-only printing** is selected.)
	Enter text or special characters in the footer. The special characters allowed for the header can also be used for the footer.

Related Topics

Printing from VT Sessions

Reflection Desktop provides full access to the printing capabilities of your Windows printer, like any Windows application. From a VT session, you can print the screen, the display memory, or just the selected text. In addition, Reflection provides a terminal emulation feature called logging, which is similar to printing.

The Difference Between Printing and Logging

It's important to understand the difference between printing output and logging output. When logging is turned on, lines are buffered immediately as they appear on the screen. This continues until you turn logging off, when the output is actually printed. This type of "printing" parallels terminal-host printing, and, typically, the host controls printing, bypassing Reflection.

The Windows printer driver is still used, unless you select **Bypass Windows print driver** from the **Print Setup** dialog box.

In this Section

Print from a VT Session

You can print using defaults, or you can choose a print range and number of copies first.

To print using default settings

1 Open a terminal session.

2 Navigate to the screen you want to print.

3 Open the Print dialog box.

The steps depend on your user interface mode (page 216).

- ◆ If you are using the Ribbon or Browser mode, click on the Quick Access Toolbar. Then, in the Print dialog box, click **Setup**.
- ◆ If you are using Classic mode, from the File menu, choose **Print Settings** or **Print Setup**

4 In the Print dialog box, click **OK**.

To print using custom settings

1 Open a terminal session.

2 Navigate to the screen you want to print.

3 Open the Print dialog box.

The steps depend on your user interface mode (page 216).

- ◆ If you are using the Ribbon or Browser mode, click on the Quick Access Toolbar. Then, in the Print dialog box, click **Setup**.
- ◆ If you are using Classic mode, from the File menu, choose **Print Settings** or **Print Setup**

The Print dialog box opens.

4 Select a Print range option:

Select	To print
Display memory	The information visible on the display, as well as any information that has scrolled off of the display and is still in memory.
Screen	Whatever you see in the terminal window.
Selection	Any selection that is highlighted in the terminal window.

5 To print multiple copies of the selected range, choose a value from the **Copies** box.

6 Click **OK**.

Related Topics

Printing Batch Print Jobs

You can configure Reflection to accumulate output from a series of print events before you print. You might want to do this, for example, if you're connected to a network printer that is temporarily inoperative—you can collect all your printed output and print it all at once when the printer is again available.

To print a batch of print jobs

1 Open the Print dialog box.

   The steps depend on your user interface mode (page 216).

     - If you are using the Ribbon or Browser mode, click 🖶 on the Quick Access Toolbar. Then, in the Print dialog box, click **Setup**.

     - If you are using Classic mode, from the File menu, choose **Print Settings** or **Print Setup**

2 In the Print Dialog box, click **Setup**.

3 Under **Multiple screens per page**, select **Close printer manually**.

   When you print with this option selected, the print output is spooled until you click **Close Printer** on the Status bar.

4 Clear the **Auto formfeed** box.

   This prevents Reflection from ejecting the page after each print event — if you're printing to a printer this saves paper; if you're printing to a file, this prevents a page break from being inserted in the output file.

   Clearing this setting can also be useful if your host program sends a series of open printer and close printer escape sequences.

Related Topics

Prevent Character Translation

Character translation is the conversion of one character set to another. You should disable character translation if the host already generates characters in the correct character set for your printer, and your printer is not configured for the default IBM PC code page 437 character set.

The **Disable printer translation** option has little, if any, effect on screen printing or logging. When Reflection receives characters from the host, it automatically converts these characters to the ANSI character set before displaying them in Windows. The translation has already taken place before you either turn on logging or print the screen contents. Therefore, this setting is only relevant for host applications that print in controller mode. In this mode, Reflection does not know in advance what the host will be sending and does not perform automatic translation.

To prevent character translation

1 Open the Print dialog box.

   The steps depend on your user interface mode (page 216).

   - If you are using the Ribbon or Browser mode, click 🖶 on the Quick Access Toolbar. Then, in the Print dialog box, click **Setup**.

   - If you are using Classic mode, from the File menu, choose **Print Settings** or **Print Setup**

2 In the Print dialog box, click **Setup**.

3 Select **Bypass Windows print driver**.

4 Select **Disable printer translation.**

   Characters will be printed exactly the way they arrive from the host.

Related Topics

- "Print Setup Dialog Box" on page 596

Logging Data

Logging copies data from display memory to the printer each time a line feed is received so that attributes, such as underline, are printed. For VT terminals, "Controller mode" captures incoming data to the printer. Typically, logging is enabled by the host. However, if you want to configure a user-initiated logging session, you can do this from the **Logging** group on the **Tools** Ribbon.

Logging serves two functions in Reflection:

- It accommodates host printing, where an application turns on logging and starts sending data to a printer, a file, or both.

- It provides user-initiated logging of terminal sessions.

You can log to a printer, a file, or a serial device. After logging is started, all printed output is directed to the option selected under **Log output to**. Output is not written to disk or sent to the printer until you (or the host) stop logging.

Host-Initiated Printing

Many VT host applications can print to printers that are not attached to the host. This type of host-initiated printing is referred to as slave printing, logging, pass through printing, auto-print, or controller printing.

Typically, host-initiated printing involves selecting the **Print** command from a host menu. To send a print job, the host transmits escape sequences to the terminal or terminal emulator, which signal that the print job should be forwarded to a printer. Reflection supports host-initiated printing and forwards the print job to the Windows default printer.

To change where the print job is sent, use the **Logging** dialog box to select a different output option.

NOTE: The **Serial device** option is not used for typical printing, even if you have your Windows printer on the serial port. This option is only used for devices on serial ports, such as bar-code readers, which need to send information back and forth between the host and the device, through Reflection.

Serial Device-to-Host Communications

Reflection supports serial device-to-host communications (also called printer-to-host, bidirectional, or printer 2-way communications). You can enable serial device-to-host communications when you want a device on a serial port (such as a printer or bar-code reader) to be able to send information to a host via Reflection.

In this Section

- "Log Data from a VT Session" on page 588
- "Logging When Reflection is in Protect Mode" on page 589
- "Enabling Serial Device-to-host Communications" on page 589
- "Logging Dialog Box" on page 591
- "Configure Serial Device Port Dialog Box" on page 592

Log Data from a VT Session

Output is not written to disk or sent to the printer until you (or the host) stop logging.

To configure logging

1   Open the Logging Settings dialog box.

    1a   Open a VT terminal session.

    1b   Open the Logging Settings dialog box as follows:

        The steps depend on your user interface mode (page 216).

User interface Mode	Steps
Ribbon	From the **Tools** ribbon, in the **Logging** group, click the **Logging > Settings** launcher:
Reflection Browser	In the search box, enter L and then, under **Actions**, select **Logging**.
TouchUx	Tap the Wrench icon and then, under **Logging**, select **Logging**.

2   Under **Log output to**, select an output option.

- To select and configure a printer, click **Print Setup**.

    -or-

- To log to a file, select **Disk**, and then type the path and filename for the output file.

3   Click **OK**.

To start logging

1   Open a VT terminal session.

2   Start logging as follows:

The steps depend on your user interface mode (page 216).

User interface Mode	Steps
Ribbon	From the **Tools** tab, in the **Logging** group, click **Start Logging.**
Reflection Browser	In the search box, enter L and then, under **Actions**, select **Start > Logging**.
TouchUx	On the menu, tap the Wrench icon and then, under **Logging**, select **Start > Logging**.

Logging When Reflection is in Protect Mode

Reflection logs data differently when it is emulating a block mode application, such as a WYSE terminal.

Under WYSE 50+ or WYSE 60 emulation, Reflection logs the data up to the cursor the moment it receives a line feed from the host. Whether the terminal is in protect mode or unprotect mode, logging in Reflection performs the same way.

Related Topics

- "Logging Data" on page 587

Enabling Serial Device-to-host Communications

When you want a bidirectional device on a serial port (such as a printer or bar-code reader) to be able to send information via Reflection, you can enable serial device-to-host communications. Most hosts automatically initiate serial device-to-host communications (via the Csi?9i control function). If you are using a host application that does not, you may also need to manually enable serial device-to-host communications.

In this Section

- "Automatically Enable Serial Device-to-host Communications" on page 589
- "Manually Enable Serial Device-to-host Communications" on page 590

Automatically Enable Serial Device-to-host Communications

You can enable serial device-to-host communications when you want a bidirectional device on a serial port (such as a printer or bar-code reader) to be able to send information to a host via Reflection. Most hosts automatically initiate serial device-to-host communications (via the Csi?9i control function).

To enable serial device-to-host communications automatically

1 Open the Logging Settings dialog box.

   1a Open a VT terminal session.

   1b Open the Logging Settings dialog box as follows:

The steps depend on your user interface mode (page 216).

User interface Mode	Steps
Ribbon	From the **Tools** ribbon, in the **Logging** group, click the **Logging > Settings** launcher: 🔲
Reflection Browser	In the search box, enter `L` and then, under **Actions**, select 📇 **Logging**.
TouchUx	Tap the Wrench icon and then, under **Logging**, select **Logging**.

2 Under **Log output to**, select **Serial device**, and then click **Configure**.

The **Configure Serial Device Port** dialog box appears.

3 From the **Port** list, select the port to which your serial device is connected.

If necessary, change the other settings for the serial connection to your device.

The **Configure** button from the **Terminal Setup Advanced Options** dialog box is equivalent to the **Configure** button from the **Logging Settings** dialog box. You can use the button from either dialog box to configure your serial device port.

4 Click **OK**.

5 If the host application needs to send data to the serial device, from the **Logging** dialog box, clear the **Printer** check box. (You can omit this step if data flows only from the serial device to the host.)

6 Click **OK**.

Related Topics

- "Manually Enable Serial Device-to-host Communications" on page 590
- "Configure Serial Device Port Dialog Box" on page 592
- "Logging Dialog Box" on page 591
- "Logging Data" on page 587

Manually Enable Serial Device-to-host Communications

Although most hosts automatically initiate serial device-to-host communications (via the Csi?9i control function), if you are using a host application that does not, you may also need to manually enable serial device-to-host communications.

To enable serial device-to-host communications manually

1 Open a VT terminal session.

2 Open the Document Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click ⬛.
TouchUx	Tap the Gear icon and then select ⬛ **Document Settings**.

3 Under **Terminal Configuration**, click **Select Terminal Type**.

4 Under **Terminal Settings**, click **Terminal Setup**.

5 Click the **Advanced** button.

6 Select the **Serial device to host** check box.

The **Configure** button from the **Terminal Setup Advanced Options** dialog box is equivalent to the **Configure** button from the **Logging Settings** dialog box. You can use the button from either dialog box to configure your serial device port.

7 Click **OK**.

Related Topics

- ◆ "Automatically Enable Serial Device-to-host Communications" on page 589
- ◆ "Configure Serial Device Port Dialog Box" on page 592
- ◆ "Logging Dialog Box" on page 591
- ◆ "Logging Data" on page 587

Logging Dialog Box

Getting there

1 Open a VT terminal session.

2 Open the Logging Settings dialog box as follows:

The steps depend on your user interface mode (page 216).

User interface Mode	Steps
Ribbon	From the **Tools** ribbon, in the **Logging** group, click the **Logging > Settings** launcher: ⬛
Reflection Browser	In the search box, enter `L` and then, under **Actions**, select ⬛ **Logging**.
TouchUx	Tap the Wrench icon and then, under **Logging**, select **Logging**.

Use this dialog box to configure logging and to enable serial device-to-host communications.

The options are:

Log Output To

Printer	Select to print the output. The printer selected in **Print Setup** is displayed.
Print Setup	Click to control printer settings that apply only to Reflection, or to select a different Windows printer.
Disk	Select to send output to a file. Type the path and filename for the output file.
	Create an ASCII text file, and translate line-drawing characters to their closest ANSI equivalent.
Serial device	Select to send output to the bidirectional serial device connected to the configured serial port. For more information, see the topic Automatically Enabling Serial Device-to-Host Communications (page 589).
	NOTE: The **Serial device** option is not used for typical printing, even if you have your Windows printer on the serial port. This option is only used for devices on serial ports, such as bar-code readers, which need to send information back and forth between the host and the device, through Reflection.
Configure	Click to select and configure a serial port.
	The **Configure**button from the **Terminal Setup Advanced Options** dialog box is equivalent to the **Configure** button from the **Logging Settings**dialog box. You can use the button from either dialog box to configure your serial device port.

Related Topics

- "Logging Data" on page 587
- "Automatically Enable Serial Device-to-host Communications" on page 589
- "Configure Serial Device Port Dialog Box" on page 592

Configure Serial Device Port Dialog Box

Getting there

The **Configure** button from the **Terminal Setup Advanced Options** dialog box is equivalent to the **Configure** button from the **Logging Settings** dialog box. You can use the button from either dialog box to configure your serial device port.

From the Logging dialog box

1 Open a VT terminal session.

2 Open the Logging Settings dialog box as follows:

The steps depend on your user interface mode (page 216).

User interface Mode	Steps
Ribbon	From the **Tools** ribbon, in the **Logging** group, click the **Logging > Settings** launcher:
Reflection Browser	In the search box, enter ∟and then, under **Actions**, select **Logging**.
TouchUx	Tap the Wrench icon and then, under **Logging**, select **Logging**.

3 Under **Log output to**, click the **Configure** button.

From the Terminal Setup dialog box

1 Open a VT terminal session and then open the Settings dialog box.

The steps depend on your .

User Interface Mode	Steps
Ribbon or Reflection Browser	With a session open in Reflection, from the **Quick Access Toolbar**, click .
TouchUx	Tap the Gear icon and then select **Document Settings**.

2 Under **Terminal Configuration**, click **Select Terminal Type**.

3 Under **Terminal Settings**, click **Terminal Setup**.

4 Click the **Advanced** button.

5 Next to the **Serial device to host** check box, click the **Configure** button.

The options are:

Port	Select the communications port to which your target serial device is connected.
Baud rate	Set the rate at which Reflection transmits and receives data through the selected serial port.
	The baud rate setting must match the baud rate of your direct connection.
Parity	Set the parity for data transmission to and from the serial device on this port.
	This setting determines whether a parity bit is generated for each character transmitted. Parity is used to detect errors in data transmission; the number preceding the slash indicates the number of data bits sent.
	To use the multinational character set or 8-bit controls, **Parity** must be set to one of the values that offers 8-bit controls. If your communications link generates parity, and you set **Parity** to **8/None**, multinational characters appear on your screen. In this case, set **Parity** to either **8/Even** or **8/Odd**.

Pacing

It is possible for Reflection to transmit data to a serial device faster than the device can process it, or for a serial device to transmit data to Reflection faster than Reflection can process it.

Should this continue for too long, the slower system's buffer overflows and data is lost. If the serial device recognizes the XON/XOFF handshake, you can prevent the buffer from overflowing by keeping this value set to **Xon/Xoff**.

Xon/Xoff transmit pacing works as follows:

- When the receive buffer has a limited amount of space left, an XOFF (DC3) character is sent as a signal to stop transmitting.
- After processing most of the backlog of characters in the receive buffer, an XON (DC1) character is sent as a signal to resume transmission.

The two systems continue in this stop-and-go fashion until all the data has been transmitted.

If **Hardware** is selected, the RTS and CTS pins on the RS-232 serial cable control data flow.

Transmit	Select a flow control method to use when Reflection transmits data to a serial device on this port.
Receive	Select a flow control method to use when the serial device on this port transmits data to Reflection.

Related Topics

- "Automatically Enable Serial Device-to-host Communications" on page 589
- "Logging Data" on page 587
- "Advanced Options Dialog Box for VT Terminal Types" on page 365

Configure Printing Options

Any configuration you perform is saved with your session document.

To configure printing options

1 Open a terminal session.

2 Open the Print dialog box.

   The steps depend on your user interface mode (page 216).

   - If you are using the Ribbon or Browser mode, click 🖶 on the Quick Access Toolbar. Then, in the Print dialog box, click **Setup**.

   - If you are using Classic mode, from the File menu, choose **Print Settings** or **Print Setup**

3 In the Print dialog box click **Setup**.

4 From the **Print Setup** dialog box, choose the settings you want, and then click **OK**.

   The settings you choose apply only to Reflection.

5 Open the Page Setup dialog box.

   Open the Page Setup dialog box as follows:

   The steps depend on your user interface mode (page 216).

   - If you are using the Ribbon or Browser mode, click 🖶 on the Quick Access Toolbar and then click **Page Setup**.

   - If you are using the TouchUx mode, tap the Folder icon and then under **Print**, select **Page Setup**.

6 From the **Page Setup** dialog box, choose the settings you want for the paper size and source, the page orientation, and the margins.

7 (Optional) Click the **Page Options** button, and then from the **Page Options** dialog box, set the font to use for printed output, specify the number of rows and columns to appear on the page, and then click **OK**.

8 From the **Page Setup** dialog box, click **OK**.

Related Topics

- "Print Setup Dialog Box" on page 596
- "Page Setup Dialog Box" on page 598
- "Page Options Dialog Box" on page 599

Print Dialog Box

Getting there

1 Open a terminal session.

2 Open the Print dialog box as follows:

- If you are using Ribbon or Browser mode, click ⎙ on the Quick Access Toolbar.
- If you are using TouchUx mode, tap the Folder icon and then under **Print**, select **Print**

The printer selected in **Print Setup** is shown on this dialog box.

Print range

Display memory	Display memory contains both the information visible on the display and information that has scrolled off of the display.
Screen	Print only what you see on the screen.
Selection	Print the currently highlighted selection.
Copies	Select the number of copies you want to print.
Print Setup	Click to control printer settings that apply only to Reflection, or to select a different Windows printer.

Related Topics

- "Print Setup Dialog Box" on page 596
- "Print from a VT Session" on page 585

Print Setup Dialog Box

Getting there

1 Open a terminal session.

2 Open the Print dialog box as follows:

- If you are using The Ribbon mode, click ⎙ on the Quick Access Toolbar and then click **Setup**.
- If you are using the Classic mode, from the **File** menu, choose **Print Settings**

Any configuration you perform is saved with your session document.

Printer

Name	Select a printer from this list of printers currently connected to your computer.
Properties	Click to set printer-specific options.
Status, Type, Where, Comment	These read-only fields describe the selected printer.

Print to file	Create an ASCII text file, and translate line-drawing characters to their closest ANSI equivalent.
Print output to	Type the path and filename for the output file.
	Unless you change the path or filename, output continues to be appended to this file each time you perform a print function.
Bypass Windows print driver	Select to send raw data (including printer control escape codes) directly to your printer. Output is sent to the printer immediately, instead of waiting for a whole page of information, and the Windows printing interface is bypassed.
	If you're bypassing Windows printing to a PostScript printer, the results may not be what you expect. PostScript printers are controlled by PostScript commands, which are typically sent to the printer from a PostScript printer driver.
	You cannot bypass the Windows print driver when you are printing to a file.
Disable printer translation	If you are bypassing the Windows print driver, you can also disable printer translation. Characters will be printed exactly the way they arrive from the host.
	You should disable character translation if the host already generates characters in the correct character set for your printer, and your printer is not configured for the default IBM PC code page 437 character set.
	The **Disable printer translation** option has little, if any, effect on screen printing or logging. When Reflection receives characters from the host, it automatically converts these characters to the ANSI character set before displaying them in Windows. The translation has already taken place before you either turn on logging or print the screen contents. Therefore, this setting is only relevant for host applications that print in controller mode. In this mode, Reflection does not know in advance what the host will be sending and does not perform automatic translation.
Print ANSI color background	By default, the ANSI background is not printed; a potential savings on printer toner because the ANSI background is often black. To reverse this, select the **Print ANSI color background** option.
	This feature is available only when printing to a printer using a Windows print driver.
Digital LA210 emulation	The LA210 is a type of Digital printer that supports a series of escape sequences for setting the number of columns and rows per page. Reflection intercepts the escape sequences and changes the font to emulate the number of columns or rows. This option controls whether Reflection translates data when a pass-through method of printing, such as printer controller mode, is being used. If your host software understands PC printers, select this option.
	This feature is available only when printing to a printer using a Windows print driver.

Auto formfeed	By selecting this option, an `FF` character is generated after a print event. Clear this option and the **Bypass Windows print driver** option if you do not want Reflection to eject the page after printing. For example, you may not want a form feed generated when you print multiple selections (using the **Selection** option under **Print > Range** in the **Print**dialog box).

Clearing this setting can also be useful if your host program sends a series of open printer and close printer escape sequences. |
| **Network** | Click to connect to a shared network printer. |

Close printer

Manually	Select to keep the printer open until you close it manually by clicking the **Close Printer** button; otherwise, the printer closes when the print job is finished.
After X seconds	Select to close the printer automatically after the amount of time you specify. The value you enter here determines how long Reflection waits after a host print job is completed before automatically closing the printer.

Related Topics

- "Configure Printing Options" on page 595
- "Print Dialog Box" on page 596

Page Setup Dialog Box

Getting there

1 Open a terminal session.

2 Open the Page Setup dialog box as follows:

   The steps depend on your user interface mode (page 216).

   - If you are using the Ribbon or Browser mode, click ⎙ on the Quick Access Toolbar and then click **Page Setup**.
   - If you are using the TouchUx mode, tap the Folder icon and then under **Print**, select **Page Setup**

The options are:

Paper

Size	Select the size of the paper or envelope you want to use.
Source	Choose the tray where the paper you want to use is located in the printer. Different printer models support different paper sources.

Orientation

Choose how the document is positioned on the page. The Page Preview at the top of the dialog box shows an example of the currently selected orientation.

Margins (inches)

Use the settings in this group box to set the printing area for the page. Reflection will not print outside the boundaries you specify. The Page Preview at the top of the dialog box shows an example of the currently selected margins.

Page Options	Open the **Page Options** dialog box, from which you can set the font to use for printed output, and specify the number of rows and columns to appear on the page.

Related Topics

- "Configure Printing Options" on page 595
- "Page Options Dialog Box" on page 599

Page Options Dialog Box

Getting there

1 Open a terminal session.

2 Open the Page Setup dialog box as follows:

The steps depend on your user interface mode (page 216).

- If you are using the Ribbon mode, on the **File** menu, mouse over **Print**, and then choose **Page Setup**.

- If you are using the Classic mode, from the **File** menu, choose **Page Setup**.

3 From the **Page Setup** dialog box, click the **Page Options** button.

Text format

Font	The default font is a TrueType font called `r_ansi`, installed by Reflection. To change the printer font, select a new name from the **Font** box. Only those fonts supported by your printer are listed.
	NOTE: You can print only using monospace TrueType fonts (also known as fixed pitched).
Use printer default font	Select to speed up printing by using your printer's built-in font.
Print inverse video	Select to print inverse screen text as inverse text; otherwise, inverse screen text is printed as normal text.
	NOTE
	◆ Your print driver must support inverse-mode printing for this feature to work.
	◆ This option is not available when **Use printer default font** is selected.

Fit font to page	When cleared, Reflection considers limiting factors of height or width when determining font size. Printed fonts are always be correctly proportioned. However, the text may not fill the printed page.
	When selected, Reflection adjusts the height and width of the font based on the page size and the number of rows and columns on the page, so that text always fills the printed page.

NOTE

- These adjustments may give the font a distorted appearance. To print the optimal amount of text per page, select the **Auto row sizing** check box.

- This option is not available when **Use printer default font** is selected.

Column dimensions

Columns per row	Changing the number of columns is useful for printing wide reports.
	NOTE: Changing the setting for **Number of characters per row** (from **Document Settings** > **Set up Display Settings** > **Dimensions**) automatically changes the printer columns.

Row dimensions

Rows per page	If the value you select here exceeds what your printer can fit on one page (this number varies from printer to printer), Reflection prints the maximum number of lines it can fit on the page.
Auto row sizing	Select to print the optimal number of rows that can fit onto a page, given the values you specified in the **Page Setup** and **Page Options** dialog boxes. If you change those values after selecting this option, Reflection automatically calculates a new optimal number of rows to be printed per page.

Related Topics

- "Configure Printing Options" on page 595
- "Page Setup Dialog Box" on page 598

View Settings Dialog Box (Printer Sessions)

Getting there

1 Open a printer session.

2 From the **Setup** menu, choose **View Settings**.

The **View Settings** dialog box lists all your current printer session settings. This list includes all settings you can configure using any printer session dialog box, and some additional settings that can only be set from the **View Settings** dialog box.

You can use the **View Settings** dialog box to check the current value of a setting, change its value, find out what values can be used, or view help for a setting. You can also find out which settings have been changed from their default values.

When you change a setting in the **View Settings** dialog box, the corresponding setting in a the printer session dialog box (if there is one) changes also. For example, if you change the value of **Auto Connect** from No to Yes, the **Auto connect** check box in the **Session Setup** dialog box is selected.

The options are:

Search	Enter text to quickly locate settings whose name includes that text.
Reflection settings	Lists printer settings. You can filter this list using the **Search** and **Display settings** options.
Display settings	Filters the list so you can view only settings that have been changed from their default values.
Setting details	Shows the value of the currently selected setting.
Help	Displays this help topic.
Setting help	Displays information about the currently selected setting.

Related Topics

Printer Emulation Settings

This list contains the printer settings available in the **View Settings (page 600)** dialog box.

In this Section

AS/400 Host Name

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

Use this setting to specify the name of the IBM System i (AS/400) host to which you want to connect when **Service Location Protocol (SLP)** is enabled. This ensures that you connect to the IBM System i (AS/400) named even if the load balancing features of SLP have connected you to an IBM System i (AS/400) running fewer sessions.

Assigned AS/400 Host

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This read-only setting specifies the IBM System i (AS/400) you're assigned to when **Service Location Protocol (SLP)** is enabled.

Assigned Device Name

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This read-only setting specifies which device is assigned for your connection. Applies to 5250 printer sessions only.

Assigned Encryption Strength

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies the encryption strength used by Secure Sockets Layer/Transport Layer Security (SSL/TLS) data stream encryption. You can specify an encryption strength or let the host negotiate an encryption strength with Reflection.

NOTE: Before you can this setting, you must enable "Telnet Encryption" on page 643.

Assigned Host Name

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This read-only setting specifies the host to which your session is connected. Applies only to Telnet connections that use Service Location Protocol (SLP).

Assigned LU Name

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This read-only setting specifies which LU (session) is assigned for your connection. Applies to 3270 sessions only.

Auto Connect

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

Select this check box to establish a host connection immediately after you open the associated settings file, and then save your settings to an *.rsf file (the changes take effect the next time you load the file).

For example, if you configure a host named TELSTAR in the **Session Setup** dialog box and select **Auto Connect**, and then choose **File** > **Save As** and save your settings to a file named Telstar.rsf, Reflection automatically connects to TELSTAR when you open the Telstar.rsf file.

Auto Reconnect

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

If **Auto Reconnect** is set to Yes, Reflection attempts to reconnect after any disconnection that is not initiated by Reflection. Applies to 5250 connections using Telnet, and 3270 connections using Telnet or Telnet Extended.

Bypass Windows Printing

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies whether to disable having Windows handle fonts, font size, font style, and lines-per-inch configuration. Affects 3812 printing and 3287 printing.

NOTE: Bypassing Windows printing is not the same as disabling Windows print spooling, which you can do from the Control Panel. Disabling print spooling is not recommended if you're printing to a network printer or running multiple applications that may be sending data to the printer.

Bypass Windows Printing in Transparent Mode

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies whether to disable having Windows handle fonts, font size, font style, and lines-per-inch configuration while in Transparent mode. Affects 3812 printing and 3287 printing.

NOTE: Bypassing Windows printing is not the same as disabling Windows print spooling, which you can do from the Control Panel. Disabling print spooling is not recommended if you're printing to a network printer or running multiple applications that may be sending data to the printer.

C/370 Character Set

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies whether to use the C/370 code page. The C/370 code page provides support for square brackets ("[" and "]").

Caption

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies the string that appears in the Reflection title bar, and is also displayed within the taskbar.

NOTE: Note :When Reflection is running, but minimized, the defines the string shown on the taskbar.

Type text and/or shortcuts up to 260 characters in the **Settings details** box.

Shortcut	Option
&w	**Micro Focus**
&r	**Reflection**
&f	Settings File Name (or **Untitled** if a settings file is not open)
&s	Session Type
&t	Transport
&h	Host Name

Shortcut	Option
&d	Date
&c	Connection Status (whether you are connected and over what transport)
&p	Printer Status (relevant only if the **Session Type** is IBM 5250 Printer or IBM 3270 Printer)
&x	Transfer Status (the percentage complete of file and data transfers)
&v	Assigned Device Name (relevant only for 5250 sessions that use an assigned Device Name)
&l	Assigned LU Name (relevant only for 3270 sessions that use an assigned LU Name)
&o	Profile Name
&&	A Single Ampersand

Command Line Switches

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This read-only setting shows the command line switches (also called command line parameters), if any, that were used to start Reflection.

Confirm on Exit

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies whether a confirmation dialog box appears if you try to exit Reflection while connected to a host.

NOTE: Changes you make to this setting are saved to the Windows registry and affect all Reflection sessions.

Country Extended Graphics Code

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

Select to make additional characters available in the configured **National character set**. See your host documentation for details.

Create Settings File Shortcut

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies whether Reflection automatically creates a shortcut whenever you save a settings file. You can use the shortcut to start Reflection and open your saved settings.

Current Display Height

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This read-only setting specifies the number of rows in the current display height.

NOTE: The value of this setting includes two non-addressable rows that are dedicated to the Operator Information Area (OIA) — the actual number of addressable rows in the display height is the number of addressable rows minus two (2).

Current Display Width

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This read-only setting specifies the number of columns in the current display width.

Current Locale

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This read-only setting shows in which language Reflection is running. Use this setting to determine which language Reflection is using when no language has been specified in either the "Locale" on page 616 or "Language Override" on page 616 settings.

Current Trace Record

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies the current trace record and is relevant only when **Pause Playback Trace on EOR** is set to Yes (default).

As you play back a trace, you can restart the trace at any point by changing the value of **Current Trace Record**. If you specify a value greater than the number of records in the trace file, trace playback stops.

Default Printer Copies

Getting there

1   Open a printer emulation session.

2   From the **Setup** menu, choose **View Settings**.

This setting determines the number of copies to print. If you write a command to print, you must specify the number of copies in the command.

Device Name

Getting there

1   Open a printer emulation session.

2   From the **Setup** menu, choose **View Settings**.

Use this setting to specify the name of the device (up to 32 characters) to which you want to connect.

NOTE: You cannot change this value while you're connected.

Enable Asynchronous Transport Behavior

Getting there

1   Open a printer emulation session.

2   From the **Setup** menu, choose **View Settings**.

This setting specifies whether Reflection reverts to polling mode for host interactions. Used primarily for diagnostic purposes.

Enable Host Alarm

Getting there

1   Open a printer emulation session.

2   From the **Setup** menu, choose **View Settings**.

This setting specifies whether the host sounds alarms (beeps) in 5250 sessions.

Font Character Set

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

Specify the character set that Reflection uses for its user interface.

Choose from the following character sets:

- Ansi Character Set (default)
- Arabic Character Set
- Baltic Character Set
- Chinese Big5 Character Set
- East European Character Set
- GB2312 Character Set
- Greek Character Set
- Hangeul Character Set

- Hebrew Character Set
- Johab Character Set
- Oem Character Set
- Russian Character Set
- ShiftJis Character Set
- Thai Character Set
- Turkish Character Set

Fully Qualified Remote LU Name

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting defines the IBM System i system in the following format:

`NetId.LuName`

Generate Device Names

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

To create device names based on the values you enter for **Device Name** from the **Session Setup** dialog box, set **Generate Device Names** to Yes. Available only for 5250 Telnet sessions.

Type any of the following characters as part of the value in the **Device Name** box:

Value	Usage
*	For each new session, replaced by "A", "B", "C", and so on. If the entire alphabet is used, the generated device names continue with "AA", "AB", "AC", and so on.
%	For printer sessions, replaced by "P"; for display sessions, replaced by "S".
=	For each new session, replaced by "1", "2", "3", and so on.
&COMPN	Replaced by the local workstation name; left-trimmed if the generated name exceeds 10 characters. **NOTE:** This character cannot be used with "&USERN".
&USERN	Replaced by the local user name; left-trimmed if the generated name exceeds 10 characters. **NOTE:** This character cannot be used with "&COMPN".
+	Use anywhere in the string with "&USERN" or "&COMPN" to specify right-trimming instead of left-trimming.

NOTE: You can use only one string literal in combination with these characters. If you use separated strings, the second string is dropped. For example, if you use "%My=Device", the second string ("Device") will be ignored when the device name is generated. However, "%MyDevice" contains only one string ("MyDevice") and won't have this problem.

Examples

This Device Name setting	Generates
"%ABC="	The device name SABC1 for a display session. If this is rejected, Reflection will try SABC2, SABC3, and so on.
"%123*"	The device name S123A for the first display session, S123B for the second session, and so on.
"&COMPN*"	The names puternameA, puternameB, puternameC for the first three sessions, when the computer name is "Computername".
"+&USERN*"	The names victorruA, victorruB, victorruC for the first three sessions, when the computer user name is "victorrubio".

NOTE: In display sessions, the device name appears in the sign-on screen when you connect to the host; in printer sessions, the device name appears in the "Assigned Device Name" on page 606 setting details in the **View Settings** dialog box.

Host Communication Timeout

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies the number of seconds Reflection should wait for a host connection response. If there is no response from the host in the allotted time, an error results.

Host Name

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

Use this setting to specify the host to which you want to connect. Type a value (up to 260 characters) to indicate an Internet address, an Internet node name, or a name that can be resolved by a Hosts file or a domain name server.

Host Network Address

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This read-only setting specifies the address of the host.

Host Print Timeout

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

Use this setting to specify the number of seconds to wait after the host stops sending data to a printer session before forcing all pending printer output to the printer. The action performed by this setting is equivalent to pressing the Flush button on the 3287 printer panel.

Hosts File Name

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

Specify the path to the Hosts file (up to a maximum of 260 characters), which maps assigned node names to Internet addresses. Reflection changes the value of this setting when it finds a Hosts file.

Reflection searches for the Hosts file in the following locations (in order):

- In the same path as Wsock32.dll
- If the System or System32 folder of the operating system's root folder
- In the folder where Reflection is installed
- The current folder
- In the operating system's root folder
- The folders in your Path statement

If Reflection cannot find the Hosts file in any of locations in the preceding list, this field remains blank. To locate a Hosts file on your PC, from the **View Settings** dialog box, select Hosts File Name and click the **Browse** button, or use the operating system's Find feature.

NOTE: Windows TCP/IP software must be able to locate the Hosts file in the Winnt\System32\Drivers\Etc folder before Reflection can generate a list of hosts.

Icon Title

Getting there

1 Open a printer emulation session.
2 From the **Setup** menu, choose **View Settings**.

Specifies the string that appears on the taskbar when Reflection is minimized. If Reflection is not minimized, the string shown on the taskbar is defined by the **Caption** setting.

In the **Settings details** text box, enter text or any of the following predefined options (up to 260 characters).

Shortcut	Option
&w	**Micro Focus**
&r	**Reflection**
&f	Settings File Name (or **Untitled** if a settings file is not open)
&s	Session Type
&t	Transport
&h	Host Name
&d	Date
&c	Connection Status (whether you are connected and over what transport)
&p	Printer Status
&x	Transfer Status (the percentage complete of file and data transfers)
&v	Assigned Device Name (relevant only for 5250 sessions that use an assigned Device Name)
&l	Assigned LU Name (relevant only for 3270 sessions that use an assigned LU Name)

Shortcut	Option
&o	Profile Name
&&	A Single Ampersand

Language Override

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

Specifies the language Reflection uses for menus, dialog boxes, and Help when a new (untitled) session is opened. When set to Off (default), language is based on your current system configuration and the Reflection language support you have installed. The same is true if you specify a language for which you have not installed support. This setting is saved to the registry, and takes effect the next time you start a Reflection session.

This setting is similar to the "Locale" on page 616 setting; however, **Locale** saves language information to a settings file. When you open a settings file, Reflection uses the current value of the **Locale** setting, whereas the **Language Override** setting affects all new sessions.

Locale

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies which language to use in the Reflection user interface and Help files. If you don't have the necessary .DLL file, this setting does not change the language used in the interface and help files. However, it does change some of the accelerator keys to those used in the localized version of the product.

This setting is similar to the "Language Override" on page 616 setting, however **Locale** saves language information to a settings file. Use **Locale** to select a language for a particular session for which you have created a settings file. Use **Language Override** to select a language for all new sessions.

Manufacturer Type

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

Use this setting to specify the printer manufacturer type that the IBM System i will use to print host print jobs when **Print Transform** is set to Yes.

The **Manufacturer Type** setting must match a manufacturer type and model defined on the IBM System i host. To select from a list of possible values, you can set this value using the "5250 Printer Device Initialization Dialog Box" on page 568.

This setting affects only 5250 printer sessions.

Maximum Internal Trace File Length (MB)

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies the maximum size for a trace file, in megabytes. If the internal trace file exceeds this amount, the oldest data is overwritten by the newer data, a process called wrapping. A setting of 0 (default) means that the trace file does not wrap but continues to get bigger for as long as the tracing lasts.

Change this setting from the default value to trace problems that are intermittent or not easily reproducible.

Menu Visible

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies whether the **Menu Bar** is displayed in the Reflection screen.

Message Library

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies which library contains the message queue for exception messages.

The default value, *LIBL, is sufficient for most cases. Consult your system administrator before changing this value.

Message Queue

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

Use this setting to specify the IBM System i message queue to which exception messages are sent. For example, the IBM System i may need to send a message to the printer to switch paper trays.

The default message queue is contained in QSYSOPR. Consult your system administrator before changing this value.

National Character Set

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies the national character set for your terminal sessions and should match the national character set used by your host system. If it does not, some characters, such as accents, may not display correctly.

See your host documentation for definitions of the characters in each set.

New Session Uses Current Session's Settings

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

When set to No (default), new sessions use the default Reflection settings; when set to Yes, new sessions use the settings and macros configured in your current Reflection session.

NOTE: The system administrator can configure the default session settings using the Reflection profiler.

New Window on Open

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies whether to open a new window when you open a settings file.

OLE Application Name

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This read-only setting returns the name of the Reflection product.

Path and Name of Executable

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This read-only setting returns the full path and filename (including the drive letter) for the Reflection executable file.

Path to Executable

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This read-only setting returns the full path (including the drive letter) for the Reflection executable file.

Print at End of Document

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

Use this setting to specify data that you want to send to the printer at the end of a document. The **Bypass Windows Printing** setting must be enabled.

When specifying data, use C Constant expressions, such as the following:

\a	bell
\b	backspace
\e	escape
\f	form feed
\n	new line
\r	carriage return
\t	horizontal tab
\v	vertical tab

Print at Start of Document

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

Use this setting to specify data that you want to send to the printer at the start of a document. Data must be formatted using the C constant format and the **Bypass Windows Printing** setting must be enabled.

When specifying data, use any of the following predefined constants:

\a	bell
\b	backspace
\e	escape
\f	form feed
\n	new line
\r	carriage return
\t	horizontal tab
\v	vertical tab

For example, the string `\e&l10\x1A\0\007` would be interpreted as [ESC]&l10[CTRL-Z][NULL][BELL].

Print Auto Orientation

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting determines the orientation from the page dimensions of a print job instead of from an explicit landscape or portrait command. Applies only to 3812 printing (setting corresponds to the automatic orientation control on a 3812 printer).

Print Auto Word Wrap

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies whether to wrap text when the end of a line is reached in a host print job.

Print Compress Font Vertically

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies whether Reflection compresses Thai characters vertically to improve legibility. Applies only to 5250 sessions running in Thai language versions of Reflection.

Print DBCS:SBCS in 2:3 Ratio

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies whether to make double-byte characters up to 1.5 times wider than their default size to make them more readable when printing host print jobs and terminal screens.

When set to Yes, Reflection expands double-byte characters so that two characters occupy the same number of spaces as three single-byte characters. Applicable to 5250 sessions only.

Print DBCS with a Smaller Font

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies whether to print double-byte characters using a smaller font size. Applies only to 5250 sessions.

Print Destination

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

Specifies the destination printer for print jobs. You can specify a printer using this setting or using the **Print Setup** dialog box.

Related Topics

◆ "Print Setup Dialog Box" on page 578

Print Device ASCII 899

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies whether the current 5250 printer session supports ASCII code page 899. Valid only if **Host Print Transform** (page 630) is selected.

Print Device Envelope Source

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies the envelope source on the host printer. Choose from the following:

Option	Description
*B5	Size B5 (176 × 250 mm) envelopes.
*C5	Size C5 (162 x 299 mm) envelopes.
*DL	Size DL (110 × 220 mm) envelopes.
*MONARCH	Monarch-sized (3.875 × 7.5 in.) envelopes.
*NONE	No source specified.
*NUMBER10	Number 10 (4.125 × 9.5 in.) envelopes.
*NUMBER9	Number 9 (3.875 × 8.875 in.) envelopes.
*SAME	Reflection uses the currently configured host value for the envelope source.
Windows printer	Reflection uses the currently configured value for envelope source specified by the default Windows printer.

Print Device Font ID

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies the Font Typestyle ID to use for printing host print jobs.

The default is typestyle ID 11 (Courier 10 point).

Print Device Forms Mode

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies how forms are fed into the printer, or the form feed type used for spooled files.

Choose from the following options:

*AUTOCUT (default)	Use when single-cut sheets are fed into the printer automatically (the printer must have the sheet feed attachment).
*CONT	Use when continuous forms are fed automatically by the printer.
*CUT	Use when single-cut sheets are fed manually into the printer.

NOTE: The value for **Paper Source 1** overrides the value for **Print Device Forms Mode** when **Host Print Transform (page 630)** is enabled.

Print Device Paper Source 1

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies the first or primary paper source to be used by the host printer.

Choose from the following options:

Option	Description
*A3	A3-sized paper (297 × 420 mm)
*A4	A4-sized paper (210 × 297 mm)
*A5	A5-sized paper (148 × 210 mm)
*B4	B4-sized paper (257 × 364 mm)
*B5	B5-sized paper (182 × 257 mm)
*CONT132	Continuous form paper (13.2 in. wide)
*CONT80	Continuous form paper (8 in. wide)
*EXECUTIVE	Executive-sized paper (7.25 × 10.5 in.)
*LEDGER	Ledger-sized paper (17 × 11 in.)
*LEGAL	Legal-sized paper (8.5 × 14 in.)
*LETTER	Standard letter-sized paper (8.5 × 11 in.)

Option	Description
*MFRTYPMODEL	When you select *MFRTYPMODEL, the IBM System i substitutes the value most common for your printer (*LETTER for page printers, *CONT132 for wide-carriage continuous-feed printers, and so on).
*NONE	No paper source is specified.
*SAME	Reflection uses the currently configured host value for the primary paper source.
Windows Printer	Reflection uses the currently configured value for primary paper source specified by the default Windows printer.

Print Device Paper Source 2

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies the secondary paper source to be used by the host printer. Choose from the following options:

Option	Description
*A3	A3-sized paper (297 × 420 mm)
*A4	A4-sized paper (210 × 297 mm)
*A5	A5-sized paper (148 × 210 mm)
*B4	B4-sized paper (257 × 364 mm)
*B5	B5-sized paper (182 × 257 mm)
*CONT132	Continuous form paper (13.2 in. wide)
*CONT80	Continuous form paper (8 in. wide)
*EXECUTIVE	Executive-sized paper (7.25 × 10.5 in.)
*LEDGER	Ledger-sized paper (17 × 11 in.)
*LEGAL	Legal-sized paper (8.5 × 14 in.)
*LETTER	Standard letter-sized paper (8.5 × 11 in.)
*MFRTYPMODEL	When you select *MFRTYPMODEL, the IBM System i substitutes the value most common for your printer (*LETTER for page printers, *CONT132 for wide-carriage continuous-feed printers, and so forth).
*NONE	No paper source is specified.
*SAME	Reflection uses the currently configured host value for the secondary paper source.

Option	Description
Windows Printer	Reflection uses the currently configured value for secondary paper source specified by the default Windows printer.

Print File Exists Action

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies what Reflection should do if it finds a PC file with the same name as the print file you are generating.

Value	Result
Append	Adds the output to the end of the existing file.
Ask User (default)	Prompts you to make a decision.
Autonumber	Creates a new file with an incremented filename.
Overwrite	Replaces the existing PC file.
Open Error	Causes the print to file action to fail (return an error) when the PC file already exists.

Print File Name

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

Use this setting to specify the name of the file to which the host print job or screen print is saved.

Print Fit Form Size

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies the size of the form that you want Reflection to fit to the currently configured form on your Windows printer. The values are all the available form sizes for Windows printers. By default, Reflection uses the paper size specified in the **Page Setup** dialog box.

Print Fit Form to Page

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies whether to print terminal screens or host print jobs to a form defined by Windows. This setting works in conjunction with the **Print FIt Form Size** setting.

When the terminal screen or host print job is printed, Reflection scales the print output to fit the user-defined form.

Print Fit to Page

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies whether to transform print jobs to maintain the relationship between the printed page (as defined by the host) and the printed page (as defined by the current Windows printer and page configuration).

Print Fit User Form Length

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies the length of the form to which you are printing via the **Print Fit User Form to Page** setting.

The value is expressed in percent reduction (less than 100%) or expansion (greater than 100%).

Print Fit User Form to Page

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies whether to print host print jobs or terminal screens to a user-defined form. When the host print job or terminal screen is printed, Reflection scales the print output to fit the user-defined form.

Use the settings **Print Fit User Form Length** and **Print Fit User Form Width** to define the form you want to which you want to print.

Print Fit User Form Width

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies the width of the form to which you are printing via the **Print Fit User Form to Page** setting.

Print Form Feed on End of Job

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies whether to send a form feed after printing a host print job.

Print Hook Enable

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

Use this setting to send LU1 (SCS) printer data to a registered printer hook COM object instead of an actual printer for processing.

Print Honor Form Feed Only in First Column

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies whether Reflection honors only form feeds that are in the first column of a print job. When this setting is No (default), all form feeds are honored, regardless of their position in the data stream.

Print Override Host Format

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies whether Reflection page formatting (characters per line, lines per page, font, and margins) is used, regardless of what the host specifies.

Print Override Orientation

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

Enable this setting to override the page orientation set by the host and instead, use the orientation currently defined in the Windows **Page Setup** dialog box. This option is applicable to both terminal and printer sessions.

In terminal sessions, page orientation is not explicitly set by the host but may be implied by the host page size. For example, by default the host page size is defined by the number of columns and rows that make up the terminal display. If the display is narrower than it is long, portrait orientation is implied. If the display is wider than it is long, landscape orientation is implied.

In printer sessions, the host may explicitly set a particular orientation in the data stream, or an orientation may be implied by the host page size, as described in the preceding text for terminal sessions.

Print Overstrike

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies whether Reflection simulates bold printing by using overstrike printing.

NOTE: Simulated bold printing may cause an undesired shift in the printing of some DBCS characters.

To disable simulated bold printing set **Print Overstrike** to No Offset.

Print Proportional Chars per Inch

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

When this setting is enabled, the number of characters printed per line is always determined by dividing the width of the page (minus the left and right margins) by the width of a single character (the value of "Printer Chars per Inch" on page 632 is therefore ignored). Affects only 3812 printing.

Print Retain Host Format

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

Specify Yes to retain the format set by the host after a print job completes. If you specify No (default), the pre-existing format is restored after a print job completes.

NOTE: This setting is ignored if **Print Override Host Format** is enabled.

Print Suppress Blank Page

Getting there

  1 Open a printer emulation session.

  2 From the **Setup** menu, choose **View Settings**.

This setting prevents blank pages from appearing in host print jobs.

Print Suppress Initial Form Feed

Getting there

  1 Open a printer emulation session.

  2 From the **Setup** menu, choose **View Settings**.

Select Yes to suppress the first form feed encountered in the data stream prior to any printable data.

Print Suppress Newlines

Getting there

  1 Open a printer emulation session.

  2 From the **Setup** menu, choose **View Settings**.

This setting specifies how Reflection handles the suppression of extra blank lines in 3270 Printing (3287 Printer Emulation).

If a line of characters goes to the rightmost edge of the printable area, an automatic new line is generated. If a new-line character (0 x 15) occurs in the data stream after an automatic new line, two new lines occur, which creates a blank line in the printout. When this setting is Yes (default), Reflection ignores the data stream new-line character so that printed output does not include a blank line.

When this setting is No, the new line is *not* ignored and blank lines are printed. (This matches the behavior seen in the IBM PComm product.)

Print Suppress Null Lines

Getting there

  1 Open a printer emulation session.

  2 From the **Setup** menu, choose **View Settings**.

This setting specifies whether lines of data that contain only null characters are suppressed in LU3 print jobs only.

Print to File

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies whether Reflection directs screen prints and host print jobs to a file instead of a physical printer.

Print Transform

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

To enable the **Print Transform** option, select IBM 5250 Printer as **Session Type** in the **Session Setup** dialog box, and then click the **Initialize** button.

When **Print Transform** is enabled on a IBM System i print device, you can specify the following parameters for the printer device:

- ◆ Manufacturer type
- ◆ Paper source 1
- ◆ Paper source 2
- ◆ Envelope source

NOTE: If you set the **Manufacturer Type** to a printer that begins with *WSCST, you must specify the Workstation Customizing Object (WSCST) name and library that the IBM System i uses to print jobs.

Print Translate EBCDIC in TRN

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies whether to print EBCDIC characters contained within the SCS TRN command.

Print Transparent

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

In transparent mode, all page format parameters (such as **Characters Per Line** and **Lines Per Page**) are ignored.

In 3812 printer sessions, select this option when the printer device is configured for **Host Print Transform**— that is, for documents (such as PCL files) that require no page formatting from Reflection or Windows.

In 3287 printer sessions, select this option for documents, such as PostScript files, that require no page formatting from Reflection.

NOTE: This setting is only relevant when "Bypass Windows Printing" on page 607 is set to Yes.

Print Transverse Orientation

This setting specifies whether to rotate a form (make transverse) compared to what the host is requesting before printing.

Applies only to 5250 printer sessions in which either the **Print Fit User Form to Page** or **Print Fit Form to Page** setting is set to Yes.

Print Proportional Lines per Inch

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

When this setting is enabled, the height of each print line is determined by the size of the selected font (the value of "Printer Lines Per Inch" on page 635 is therefore ignored). Affects both 3812 printing and 3287 printing.

Printer Case

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies how to handle cases in a print job. Select Dual Case (default) to print the host print job using a mixture of uppercase and lowercase letters; select Upper Case to force all text in the host print job to uppercase letters.

Printer Chars per Inch

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies the number of characters to print per inch.

If "Print Proportional Chars per Inch" on page 628 is set to Yes, **Printer Chars Per Inch** is disregarded. In this case, the number of characters printed per inch is determined by the current printer font.

As you change **Printer Chars Per Inch**, "Printer Chars per Line" on page 632 may change as well; more characters per inch means more characters on a line (assuming the left and right margins don't change).

Printer Chars per Line

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies the maximum number of characters that can be printed on a single line for 3812 and 3287 printing. If the host passes down a line that exceeds the maximum, Reflection automatically wraps the line.

Depending on your printer driver, font, and font size, the actual number of characters that can be printed on a line can vary. Use the **Info** button in the printer panel to find out the number of columns you can actually print.

As you change **Printer Chars Per Line**, "Printer Chars per Inch" on page 632 may changes as well; more characters on a line means more characters per inch (assuming the left and right margins don't change).

Printer DBCS Character Rotation Angle

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies whether to rotate characters 270 degrees when printing host print jobs or terminal screens. Rotating characters 270 degrees presents host print jobs containing double-byte characters in traditional, up to down, left to right alignment.

Applies only to double-byte character sets in 5250 sessions.

Printer DBCS Horizontal Font Size

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies whether Reflection doubles the horizontal size of double-byte characters when it prints host screens or print jobs to make them more legible. Applies to 5250 sessions only.

Printer DBCS Vertical Font Size

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies whether Reflection doubles the vertical size of double-byte characters when it prints host screens or print jobs to make them more legible. Applies to 5250 sessions only.

Printer Default Font

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies font information to the Windows printer driver only when "Bypass Windows Printing" on page 607 is set to No.

Enter a string (up to 260 characters) that specifies valid font information for your current Windows printer driver. For example:

```
Courier, 10
```

Printer Default Horizontal Tab

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies the number of spaces to use for horizontal tabs. Applies to 3287 print jobs only.

Printer Default Vertical Tab

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies the number of lines to use for vertical tabs. Applies to 3287 print jobs only.

Printer Emulate FF with LF

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies whether Reflection should simulate a form feed by issuing line feeds until the end of the page is reached.

Printer Flush on End of Job

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies whether an in-progress print job is closed if an end of job condition is sent from the host.

Printer Flush on End of Media

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

Select Yes to terminate LU3 print jobs if Reflection encounters an End of Media character.

Printer Flush on Form Feed

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

Select Yes to terminate LU3 print jobs if Reflection encounters a form feed.

Printer Host LU Name

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

Specify a name (up to 32 characters), if the host requires that you supply a host LU name when connecting as a 3287 printer.

NOTE: You cannot change this value while you're connected.

Printer Line Spacing

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies the amount of space between lines for 3812 and 3287 printer output.

Option	Description
.5 Space	Output spacing is one-half line. Applies to 3812 printing only.
Single Space (default)	Output is single-spaced. Applies to both 3812 and 3287 printing.
1.5 Space	Output spacing is one and one-half lines. Applies to 3812 printing only.
Double Space	Output is double-spaced. Applies to both 3812 and 3287 printing
2.5 Space	Output spacing is two and one-half lines. Applies to 3812 printing only.
Triple Space	Output is triple-spaced. Applies to 3812 printing only.

Printer Lines Per Inch

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies vertical spacing for printer output, measured in Lines Per Inch (LPI).

Printer Lines Per Page

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

Specifies the number of lines to print on a page for 3812 and 3287 printing.

Depending on your printer driver, font, and font size, the actual number of characters that can be printed on a line can vary. Use the **Info** button in the Reflection 3287 printer panel or 3812 printer panel to find out the number of lines per page your printer driver can accommodate for the current font and font size.

As you change this value for a 3812 printer session, the value for "Printer Lines Per Inch" on page 635 may change as well; more lines on a page means more lines per inch (assuming the top and bottom margins don't change).

Printer Margin Bottom

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies the size of the margin at the bottom of a page of printed output. The units of measure are *twips*. (A *twip* equals one twentieth of a point. There are 1440 twips to an inch.)

As you change your top or bottom margin, the value for "Printer Lines Per Page" on page 635 may change as well — larger margins mean fewer lines per page.

Printer Margin Left

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies the size of the margin at the left side of a page of printed output. The units of measure are *twips*. (A *twip* equals one twentieth of a point. There are 1440 twips to an inch.)

As you change your left or right margin, the value for "Printer Chars per Line" on page 632 may change as well — larger margins mean fewer characters per line.

Printer Margin Right

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies the size of the margin to be left at the right side of a page of printed output. The units of measure are *twips*. (A *twip* equals one twentieth of a point. There are 1440 twips to an inch.)

As you change your left or right margin, the value for "Printer Chars per Line" on page 632 may change as well — larger margins mean fewer characters per line.

Printer Margin Top

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies the size of the margin at the top of a page of printed output. The units of measure are *twips*. (A *twip* equals one twentieth of a point. There are 1440 twips to an inch.)

As you change your top or bottom margin, the value for "Printer Lines Per Page" on page 635 may change as well — larger margins mean fewer lines per page.

Printer Maximum Chars per Line

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies the value that Reflection provides to host applications that ask for the maximum number of printer characters per line.

Printer Maximum Lines per Page

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies the value that Reflection provides to host applications that ask for the maximum number of printer lines per page.

Printer Orientation

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies the default page orientation used to print both host print jobs in printer sessions, and host printing from terminal sessions.

Option	Description
Default Orientation	Uses the orientation defined by the currently selected Windows printer.
Landscape Orientation	Sets the page orientation to landscape mode (for example, 11" x 8.5").
Portrait Orientation	Sets the page orientation to portrait mode (for example, 8.5" x 11").

Printer Output Reduction

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

When enabled, this 3812 printing option does the following:

- Prints in landscape orientation — that is, with the longer (11 1/2 inch) edges of the paper as the top and bottom margins, and the shorter (8 inch) edge as the left and right margins

- Reduces the height of each line to 70 percent of the Lines Per Inch value

- Sets the top and left margins to 0.5 inches
- Increases the density of printed text to 125 percent of the **Printer > Characters Per Inch** value

Printer Paper Size

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies the paper size to use for the current default Windows printer.

Printer Paper Source

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies the paper source to use for the current default Windows printer.

Printer SO/SI Presentation

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies the way Reflection treats shift-out and shift-in (SO/SI) characters, when printing host print jobs or terminal screens, in 5250 sessions only. Choose from the following:

Option	Description
SO/SI Rendered as Blanks (default)	Prints SO/SI characters as blank spaces. Select for WYSIWYG printing.
SO/SI Removed	Removes SO/SI characters and the cells they occupy, and condenses the remaining text.
	NOTE: Removing cells containing SO/SI characters changes the spacing of the text and may cause columns to go out of alignment.
SO Removed, SI Rendered as 2 Blanks	Removes SO characters, shifts double-byte characters one cell to the left, and prints SI characters as two blank spaces. This option preserves the alignment of columns in host print jobs.

Representation of Unmapped DBCS Character

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

In double-byte sessions, this setting determines how double-byte host characters not available in the Shift-JIS DBCS character translation table appear on the terminal screen, in file transfers using JISCII translation, and in printed output.

Save Changes on Exit

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies the way to handle changes to settings and macros when you exit the current session or open a new session in the current window. Choose from the following options:

Option	Description
Ask	If settings or macros have been changed, Reflection opens a dialog box from which you can save the changes, exit without saving, or cancel and return to the Reflection session.
No	Reflection closes without saving any changes.
Yes	Reflection saves any changes without prompting.

Save Window State

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies whether to save the size and position of the terminal window when you save a settings file.

NOTE: When running in a browser, Reflection cannot save the terminal window's size and position.

Settings Changed

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This read-only setting indicates whether changes to Reflection macros or settings have not been saved.

Settings File

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This read-only setting returns the name of the open settings file. If no settings file is open, an empty string ("") is returned.

Settings Update Type

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting determines which settings Reflection includes when you save a settings update file.

When you create an update file, Reflection compares your current settings to a default configuration, and saves only those settings that have been changed from their default values. Because system administrators can customize Reflection, your site defaults may differ from the Reflection factory defaults.

This setting also determines whether the default settings used for this comparison are the Reflection factory defaults, or if they are defaults that have been customized (profiled) for your site by a system administrator.

Shortcut Folder

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies the location where Reflection creates the linked shortcut when you save a settings file.

Show Status Bar

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies whether to display or hide the Reflection status bar.

NOTE: When the status bar is hidden, you cannot use the Reflection command line.

Show Title Bar

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies whether the title bar appears in display sessions.

Startup Settings

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This read-only setting specifies the name of the startup settings file.

Startup Working Directory

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This read-only setting specifies the working directory for the current session.

Status Bar Text

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies the string that appears in the status bar. Type shortcuts or text in the text box, up to 260 characters.

Shortcut	Option
&w	Micro Focus
&r	**Reflection**
&f	Settings file name (or **Untitled** if a settings file is not open)
&s	Session type
&t	Transport
&h	Host name
&d	Date

Shortcut	Option
&c	Connection status (whether you are connected and over what transport)
&p	Printer status (relevant only if the session type is IBM 5250 Printer or IBM 3270 Printer)
&x	Transfer status (the percentage complete of file and data transfers)
&v	Assigned device name (relevant only for 5250 sessions that use an assigned device name)
&l	Assigned LU name (relevant only for 3270 sessions that use an assigned LU name)
&o	Profile name
&&	A single ampersand

Support 3270 Partitions

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies whether to send the partition-related information from the terminal to the host in response to a host query request. Use this setting in 3270 sessions for host applications that are not designed to handle terminals that support partitions.

When set to Yes, the terminal includes partition-related information in its response to a host query request; when set to No (default), the terminal does not include partition-related information in its response to a host query request.

NOTE: You cannot change this setting during a connection.

Support Asian Double-byte Features

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies whether support for double-byte features is enabled. Applies only to double-byte 3270 sessions.

Telnet Average Keep Alive Roundtrip

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This read-only setting displays the average amount of time Reflection has waited for a response to a Timing Mark Command.

Telnet Encryption

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

Telnet Encryption configures Reflection to use Secure Sockets Layer/Transport Layer Security (SSL/TLS).

If **Telnet Encryption** is enabled, but your host does not support TLS, Reflection will attempt to use SSL instead. If your host supports neither SSL nor TLS, an error message appears when you try to connect, and your connection attempt will fail.

NOTE: Reflection does not support TLS client authentication.

Telnet Encryption Disable CRL Checking

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies whether Reflection checks for certificate revocation when validating host certificates in SSL/TLS Telnet sessions.

When this setting is Yes, Reflection does not perform CRL checking.

NOTE: Disabling CRL checking increases your security risk.

Telnet Encryption Strength

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies the encryption strength for Secure Sockets Layer/Transport Layer Security (SSL/TLS) data stream encryption. To configure this setting, you must enable "Telnet Encryption" on page 643.

When set to **Recommended**, the encryption strength is established by the host and Reflection during handshaking. If you set encryption strength to a specific value, the server must support this encryption level. If the server does not support the specific level, the connection is not established. If you are running in FIPS mode and select **Recommended**, Reflection negotiates using only FIPS-compliant encryption levels.

Telnet Encryption Use OCSP

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

When this setting is enabled, an Online Certificate Status Protocol (OCSP) responder checks the revocation status of digital certificates any time you try to establish a secure connection.

Telnet Encryption Verify Host Name

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies the way Reflection handles SSL/TLS Telnet connections when the host name in the certificate does not match the host being contacted. When this setting is Yes (the default and recommended value) the host name in the certificate must match the host you are contacting.

This setting is only relevant if "Telnet Encryption" on page 643 is enabled.

Telnet Environment

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

When you establish a 5250 terminal or printer session, specific information is sent to the IBM System i host to configure your session. When you connect over Telnet, you can pass additional information at connect time as input to an Exit program on the IBM System i. Use the **Telnet Environment** setting to send this additional information. Enter a string of up to 260 characters, using the following format:

```
keyword=value; keyword=value; keyword=value
```

Using Telnet Environment with Auto SignOn

When **Auto SignOn** is set to Yes, Reflection automatically signs on to the host using the current user name and password. You can set **Telnet Environment** to specify additional, non-default sign-on options using any of the following keywords in the Exit program string:

This keyword	Sets	Equivalent Sign-on Menu Option
IBMPROGRAM	The program to call.	Program/procedure
IBMIMENU	The initial menu.	Menu
IBMCURLIB	The current library.	Current library

NOTE: Because this information is sent at the time you connect, you cannot change this setting while you are connected.

Telnet Keep Alive Packets

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

By sending Keep Alive packets, you can learn about Telnet connection problems as they occur and avoid losing entered data. If you select None, no packets are sent and connection problems are communicated only when Reflection attempts to send data to the host.

Telnet Keep Alive Timeout

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting determines the interval (in seconds) between the Keep Alive packets (requests) sent by Reflection.

Telnet Location

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies where the connection originated. Use this optional setting to provide information to the host from the PC. Usage conventions vary by site.

NOTE: You cannot change this value while you're connected to a gateway.

Telnet Port

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

Specifies the host port that the Telnet session should use. The default is 23.

Telnet Protocol

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This read-only setting specifies the Telnet protocol that Reflection uses to communicate with the host. The value of this setting can change during a session. Following is a list of Telnet protocols:

Protocol	Description
NVT	The Network Virtual Terminal protocol is in use.
TN3270	Standard TN3270 protocol is in use.
TN3270E	Extended TN3270 protocol (RFC 1647) is in use.
OCS	OCS Printing protocol (RFC 1646) is in use.
TN5250	Standard TN5250 protocol is in use.

Telnet Response Mode

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies whether the PC returns a message after it receives a message from the host.

For improved performance, set this to No.

Telnet Use HTTP Proxy Server

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies whether to connect to a host through an HTTP proxy server.

Telnet Use Reflection Security Proxy

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

When SSL/TLS security is enabled and this setting is Yes, Reflection makes secure SSL connections via the Reflection Security Proxy.

Telnet Use SOCKS Proxy Server

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies whether to connect to a host through a SOCKS proxy server.

TN Association Use TerminalCx

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

Select this setting to force the printer to use the same host name that is used in the associated display session.

NOTE: If this setting is not selected, the printer uses the same host name and port as the display session.

TN3270 Primary Same as Alt

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

Select this setting to use the same model type for both primary and alternate screen sizes. When selected, you can use a model type other than model 2 for primary screens.

TN3287 Connect Type

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting determines whether the selected LU name is paired with a specific printer device in 3270 sessions only.

Select Associate if the selected LU name is paired with a specific printer device; otherwise, select Connect (default) if the selected LU name is not paired with a specific printer device.

TN Association

Getting there

1   Open a printer emulation session.

2   From the **Setup** menu, choose **View Settings**.

This setting identifies a 3270 terminal session on the host. Use this option to associate a 3270 terminal session with a specific 3270 printer session.

Related Topics

◆   "Associate a 3270 Printer Session with a Terminal Session" on page 555

Toolbar Mode

Getting there

1   Open a printer emulation session.

2   From the **Setup** menu, choose **View Settings**.

This setting specifies whether the toolbar is attached to one of the margins of the terminal window and, if so, to which margin it is attached.

Choose from the following:

This option	Attaches the toolbar to
Bottom Bar	The bottom margin of the terminal window.
Floating	N/A — the toolbar is free floating.
Left Bar	The left margin of the terminal window.
Right Bar	The right margin of the terminal window.
Top Bar (default)	The top margin of the terminal window.

Toolbar Tether

Getting there

1   Open a printer emulation session.

2   From the **Setup** menu, choose **View Settings**.

This setting specifies whether the toolbar location is tied to the terminal window location. This setting is applicable only if "Toolbar Mode" on page 648 is set to Floating.

When you set **Toolbar Tether** to Yes (default), the toolbar tracks the nearest corner of the terminal window, and moves if you move or resize the terminal window.

Toolbar Visible

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies whether the toolbar is visible.

Trace Buffer Size (KB)

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies whether Reflection uses a buffer when writing to a trace file, and if so, the size of that buffer (in kilobytes). By creating a trace buffer, you can speed up the trace. However, if Reflection shuts down unexpectedly, some trace data may not be written to the trace file.

When set to 0 (default), no buffer is used during tracing. Reflection opens the trace file, appends the data, and then closes the trace file for each trace record. When set to greater than zero, trace data is written first to the trace buffer and then copied to the trace file on disk when the buffer is full. The trace file is closed only after the trace is stopped.

NOTE: The buffer size is calculated after compression. This means that if **Trace Buffer Size** is set to 100 and "Trace Compression Type" on page 649 is set to use Huffman compression (default), approximately 200 KB of data will be transmitted before the data is written to the trace file.

Trace Compression Type

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies which compression, if any, is used when Reflection creates a trace file.

Choose from Huffman (default), None, or Runlength.

Transport Name

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This read-only setting specifies the transport currently selected in the **Session Setup** dialog box.

Use Internet Protocol Version 6

Getting there

   1 Open a printer emulation session.

   2 From the **Setup** menu, choose **View Settings**.

This setting specifies whether Reflection uses version 6 of the Internet Protocol.

Use Printer Fonts Only

Getting there

   1 Open a printer emulation session.

   2 From the **Setup** menu, choose **View Settings**.

This setting specifies whether Reflection prints host jobs using only resident fonts on the host printer.

User Data Directory

Getting there

   1 Open a printer emulation session.

   2 From the **Setup** menu, choose **View Settings**.

This setting specifies the folder where user-created files, like settings files and trace files, are saved by default.

Version String

Getting there

   1 Open a printer emulation session.

   2 From the **Setup** menu, choose **View Settings**.

This read-only setting shows the version information for your copy of Reflection.

Workstation Customizing Object Library

Getting there

   1 Open a printer emulation session.

   2 From the **Setup** menu, choose **View Settings**.

This setting specifies the library on the IBM System i that contains the Workstation Customizing Object.

Workstation Customizing Object Name

Getting there

1 Open a printer emulation session.

2 From the **Setup** menu, choose **View Settings**.

This setting specifies the Workstation Customizing Object on the IBM System i that contains information about the ASCII printer you use.

8 Creating and Using Macros

In Reflection, you can create and run macros to simplify and automate routine tasks. You can create two types of macros:

- **Visual Basic for Applications (VBA) macros** Create VBA macros when you want to interact with multiple sessions or external applications, such as Microsoft Excel. You can record VBA macros or create them in the Visual Basic editor. You don't need to know how to program to record and playback a macro but recorded macros have limitations (for example, you cannot record interaction with other applications or Web sites).

   To create complex macros that perform Reflection actions and interact with other applications, you'll need to use the Visual Basic Editor. A common approach for creating a macro is to record it and then fine-tune it using the editor. For more information about editing and programming macros, see the Reflection VBA Guide (**Help** > **VBA Guide**).

- **Express Macro Language (EML) macros** Create an Express macro when you need to automate basic tasks but are not familiar with programming or when you want to run the macro in other Micro Focus products. Express macros can be used to automate basic tasks that apply to only one session. They cannot interact with other sessions or external applications. After you create and save an Express macro, you can run it in other Micro Focus products.

   You do not need to know anything about programming syntax to create an Express macro. You can record macros or you can use the Express visual programming editor. Using this editor, you can create or edit macros by arranging graphical elements that represent code blocks rather than specifying them textually.

You can also run macros created in other products, such as Extra!, Rumba, IBM Personal Communications, Brandon Systems Jolly Giant, and Hummingbird.

Video

▶❙ Use the Macro Panel(1:52)

▶❙ How to Record a Macro When Using the Reflection Desktop Ribbon(1:14)

▶❙ How to Record a Macro When Using the Reflection Desktop Classic Interface(2:31)

▶❙ Running Extra! Macros Reflection Desktop (3:06)

- "Running VBA Macros" on page 654
- "Recording and Deleting VBA Macros" on page 655
- "Creating, Editing, and Running Express Macros" on page 657
- "Recording Complete Dialog Box" on page 658
- "Set up VBA References" on page 659
- "Using Macros Created with other Products" on page 660

Running VBA Macros

You can run VBA macros saved in your session document file from the Macro Panel. This is a convenient way to keep track of and run your macros without adding buttons to the ribbon. You can also run other types of macros from this panel after you run them from the Run Macro dialog box.

Running Macros With the Macro Panel

You can use the Macro Panel to run VBA macros saved in your session document file or to run other macros, such as referenced macros, EML macros, or macros created with other products, that you have previously run on that session. The Macro Panel is a convenient way to keep track of and run macros that apply to a session without adding buttons to the ribbon. It displays only the macros that apply to the session that has focus.

The Macro Panel has three tabs:

The Available tab shows the VBA macros that are saved in the session document file.

NOTE: The Available tab does not show EML macros, macros created with other products, or other macros that are not saved in the session document file.

The Recent tab shows all macros that you have previously run in this session. This includes VBA macros as well as other supported macros that you have run, such as EML macros or macros created with other products.

The Favorites tab shows the all the macros that you have marked as favorites.

Video

▶️ Use the Macro Panel(1:52)

Running Macros from the Run Macro Dialog Box

You'll need to use the Run Macro dialog box to run macros that are not saved in the session document file the first time you run these macros. After you run a macro once, you can run it from the Macro Panel's Recent tab.

To run a macro from the Run Macro Dialog Box

1 Open the Run Macro dialog box.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Session** tab, from the **Macros** group, click **Run Macro**.
Classic and Classic MDI	On the **Macro** menu, choose **Macros**.

2 Select the type of macro you want to run and select to open it.

   The macro runs.

   NOTE: After you run the macro once, you can run it from the Macro Panel's Recent tab.

Recording and Deleting VBA Macros

You can record a VBA macro to automate your interaction with host applications, including:

- Sending data to, or typing text in, a host application.
- Cutting, copying, or pasting text or data from one host application to another.
- Switching tabs to move from one host application to another.
- Selecting text with a mouse or clicking the mouse to move the cursor (mouse clicks are recorded as cursor positions.)

You cannot record:

- Interaction with Reflection settings and Productivity features (such as Spell Check, Auto Expand, and Auto Complete).
- Connecting to or disconnecting from a host.
- Interaction with Web applications.
- Cutting or pasting from a host to an external application (for example, Notepad).

Best Practices for Recording Macros

Use the following best practices to carefully record your macro will help prevent problems that can occasionally occur when using a slower network connection. Typing very fast while recording or "typing ahead" in a session, while connected with a slow network connection can cause your macro to play back in unexpected ways. Following these best practices will lead to the best results.

 ◆ Plan in advance of the recording to make sure you know the steps you will follow, which keys you will press, and which host screens are anticipated.

 ◆ While recording the macro, after pressing a key to submit data to the host, wait for the next host screen to fully appear (sometimes even waiting a few extra seconds) before pressing the next keys.

 ◆ If your macro doesn't play back like you expect, delete the macro and carefully record it again using slow and deliberate steps.

Recording a macro slowly and carefully does not cause the macro to run with reduced performance, as macros always run at the fastest speed possible during playback. Recording a well thought out and planned macro will lead to the best results.

To record a macro

1 **Select Record Macro**.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Macros** tab, from the **Advanced** group, click **Record VBA**.
Reflection Browser	On the **Reflection** menu, choose **Tools**, **Macro** and then **Record VBA Macro**.
TouchUx	Tap the Wrench icon, and then under **Macro**, select **Record VBA Macro**.

2 Perform the task(s) that you want to automate.

3 (Optional) If you need to interrupt the recording to perform another task, click **Pause Recording**. When you are ready to resume recording, click **Pause Recording** again.

4 When you are finished recording the macro, click **Stop Recording**.

   The **Recording Complete** dialog box appears.

5 Name the macro and choose the location where you want to save it.

6 If you want to run the macro every time the session connects, select **Make this the Connect Macro**.

   NOTE: You can fine-tune recorded macros by using the Visual Basic Editor. For more information, see Edit a Macro. (page 94)

7 If your macro doesn't play back like you expect, delete the macro and follow best practices to carefully record the macro again.

To delete a macro

1 Open the Run Macro dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Session** tab, from the **Macros** group, click **Run Macro**.
Classic and Classic MDI	On the **Macro** menu, choose **Macros**.

2 Select Reflection Workspace Macro.

3 In the Macros dialog box, select the macro you want to remove and then click **Delete**.

Video

▶️ How to Record a Macro When Using the Reflection Desktop Ribbon(1:14)

▶️ How to Record a Macro When Using the Reflection Desktop Classic Interface(2:31)

Creating, Editing, and Running Express Macros

Express Macros are general purpose macros that are supported by a number of Micro Focus products including: Reflection Desktop, InfoConnect Desktop, ZFE, and Rumba. After you create an Express macro, you can run it on any supported Micro Focus product (no editing is required).

If you are new to programming, you'll probably find it easier to get started with Express macros than you would with other languages such as Visual Basic for Applications. The Express Macro Language (EML) has a visual editor that allows you to write or edit programs by arranging code blocks. You don't have to worry about code syntax errors like missing semicolons. Instead, you can just focus on the logic of the macro to get the automation result you want.

From Reflection Desktop, you can:

- Record host interactions in an Express macro.
- Edit recorded macros or create new macros using the Express Macro visual block programming editor.
- Select and run Express macros.

Recording Express Macros

You can record a macro to automate your interaction with host applications, including:

- Sending data to, or typing text in, a host application.
- Copying and pasting text or data on a single line from one host application to another.
- Selecting text with a mouse or clicking the mouse to move the cursor. (Mouse clicks are recorded as cursor positions.)
- Connecting to or disconnecting from a host.

You cannot record:

- Interaction with Reflection settings and Productivity features (such as Spell Check, Auto Expand, and Auto Complete) or Reflection actions (for example, Open, New, or Print).

- Interaction with Web applications.

- Cutting or pasting from a host to an external application (for example, Notepad).

- Switching tabs to move from one host application to another.

NOTE: Some actions are recorded differently than might be expected:

- Only the first line of a multi-row selection is recorded. When commands such as Ctrl+A, Ctrl+Clear, Shift+Up, Shift+Down are used, the recorded macro selects only characters on the first row of the selected area.

- Ctrl+X is recorded as a Copy command instead of as a Cut command.

To record, edit, or run Express macros

- Select the button or menu commands to record, edit, or run Express macros, depending on which user interface option you are using:

If you are using this interface option	You can find these commands...
The Reflection Ribbon	On the **Macros** tab, in the **Express Macros** group.
The Reflection Browser	On the **Reflection** menu, under **Tools**, **Macro**.
TouchUx	On the Wrench icon menu.
Classic or Classic MDI	On the **Macro** menu.

NOTE: Express macros are saved as `.js` files. By default, they are saved in the Macros\Express folder in the user data directory.

Recording Complete Dialog Box

The Recording Complete dialog box automatically appears after you stop recording a macro.

From this dialog box, you can name and save the actions you've recorded as a Reflection Workspace macro.

Save in the current document's project	Saves the macro in the current session document, which must be opened each time you want to run the macro.
Save in the common project	Saves the macro in the Common project, which can be accessed from any session document on the local computer.

Macro name	Specify a unique name with no spaces. For other tips on naming Visual Basic macros, see "Naming Macros" on page 96.
	The name you specify appears after the module name in the **Run Macro**dialog box when you select a macro to run. For example, recorded macros are saved as "Recorded. *Macroname.*"
Copy script to clipboard	Saves the macro to the system clipboard, which allows you to paste it in a text file or another application.
Make this the Connect Macro	Specifies to run the macro every time the session connects.

Set up VBA References

Getting there

1 Open the Reflection Settings window as follows:

   ◆ If you're using the Ribbon interface, from the Quick Access Toolbar, click .

   ◆ For an IBM session in the Classic interface, choose **Settings** from the **Options** menu.

   ◆ For a VT Session in the Classic interface, choose **View Settings** on the **Setup** menu.

2 Under **User Terminal Configuration**, select **Set Up VBA References**.

You can centrally manage VBA macros by saving them in session document files that reside on a network share or other location and then configuring local session documents to reference these shared documents. The shared documents can reside on any location, as long as it is a trusted location.

When a local session document file with a reference to a shared session document file opens, it downloads the latest versions of the macros in the shared session document.

Reflection Desktop supports shared VBA macros for IBM (`.rd5x` and `.rd3x`) and VT (`.rdox`) session documents. You'll need to create at least one session document file for each type of terminal you are using. Session document files can only reference macros in the same type of session document. For example, IBM3270 sessions can only reference session documents with an `.rd3x`extension.

NOTE: When Reflection is unable to open a referenced session document, an error symbol is displayed next to that document. Your session cannot run macros in this file until you correct the problem.

To set up a reference to a session document file

1 In the Specify Trusted Locations dialog box, make sure the location you are saving the shared session documents on is on the list of trusted locations and add it if necessary. You must use a UNC path to specify this location. If you are using a network share, you'll also need to select **Allow trusted location on my network**. (See *"Specify Trusted Locations Dialog Box" on page 426*.)

2 Add the shared session file document names to the **Referenced Session Documents** list.

NOTE: If you are saving the shared session documents on a network share, you'll need to specify the location with a UNC path. Mapped letter drives are not supported.

---

3 Deploy the local session document as well as any trusted location settings you configured to users.

> **NOTE:** For more about setting up and deploying shared macros, see *Set up Shared VBA Macros* in the Reflection Deployment Guide.

To handle problems with references

1 If the   button is displayed next to a referenced session document, mouse over the button for information about the problem.

2 After you correct the problem (typically a missing file or a disconnected network drive), close and reopen your session.

> **NOTE:** Another way to share VBA macros is to save them in the `SharedMacros.rd3x`, `SharedMacros.rd5x`, or `SharedMacros.rdox` files and then deploy them to the user data folder. When a session opens, it automatically loads the macros from the `SharedMacros` file that corresponds to its file type. (See *Centrally Manage VBA Macros* in the Reflection Deployment Guide.)

Using Macros Created with other Products

In Reflection, you can run VBA macros created in Reflection, and most macros created with Extra! and legacy Reflection products. You can also run the majority of macros created with the Micro Focus Rumba, IBM Personal Communications, OpenText HostExplorer, and Brandon Systems\Jolly Giant QWS3270 products.

In addition, Reflection provides tools for editing Extra! Basic and Reflection Basic macros.

For more information, see the Reflection Administrator's Reference.

Video

 Running Extra! Macros Reflection Desktop (3:06)

In this Section

Legacy Reflection Macros

Reflection supports the following macro file formats:

* Settings files (.rsf,.r2w,.r4w)

- SharedMacros (.rma)
- Reflection Basic scripts (.rbs)
- Reflection Command Line scripts (.rcl)

You can open a settings file in the workspace, or run legacy macros as an external file. You can only run RCL scripts when a VT session document is active in the workspace.

To run a legacy Reflection macro

1 (Recommended) If your legacy macro was created in Reflection 10.x or earlier, save it in Reflection 14.x.

2 Open Workspace Settings.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the File menu or the Reflection button ⚙ (if using the Office 2007 Look and Feel), choose **Reflection Workspace Settings**.
Reflection Browser	On the Reflection menu, choose **Settings** and then **Reflection Workspace Settings**.
TouchUx	Tap the Gear icon and then select **Reflection Workspace Settings**.

3 Under **Trust Center**, click **Set Up API and Macro Security**.

4 From the **Legacy API preference** menu, select **Reflection**, and then click **OK**.

5 On the **Session** ribbon, click the **Run Macro** button.

6 From the **Run Macro** dialog box, specify the legacy macro that you want to run.

NOTE: If the macro contains unsupported objects, its functionality may be limited or it may not run. For a list of unsupported objects and methods, see the Reflection VBA Guide (**Help** > **VBA Guide**). If your legacy macros use early binding, and if they return compiling errors when you run them, change their Reflection namespace references from `Reflection` to `ReflectionCOM.`

Related Topics

- "Running macros created in other products" on page 90

Adding Macro Data

If you want to enter macro data each time you run a legacy Reflection macro, you can run the legacy macro from an external file by clicking the **Run Macro** button on the Ribbon, and then selecting **Legacy Reflection Macro in Another File**.

Or, you can set up an action to run legacy macros in sessions that are currently open in the workspace. To do this, create a control (such as a button or a keystroke) and associate it with the **Run Embedded Macro with Data** action.

Editing Legacy Reflection Macros <User Guide>

You can edit legacy Reflection macros in the Visual Basic Editor. However, some Session methods and properties are no longer supported. For more information, see the Reflection VBA Guide (**Help** > **VBA Guide**).

To edit a legacy Reflection macro

1 Open the settings file that contains the legacy macro.

 -or-

 If you've previously saved a settings file that contains one or more legacy macros to a Reflection session document, open the session document.

2 Open the Visual Basic Editor.

 The steps depend on your .

User Interface Mode	Steps
Reflection Ribbon	From the **Macros** tab, click **Visual Basic**.
Reflection Browser	On the **Reflection** menu, choose **Tools**, **Macro** and then **Visual Basic**.
TouchUx	Tap the Wrench icon and then under **Macro**, select **Visual Basic**.

3 In the Project pane, locate the project named ProjectLegacy(*filename*), open the appropriate module, and then edit the macro.

 NOTE: Edits to legacy macros must be done in the legacy project (ProjectLegacy).

4 Save the file as a Reflection session document to retain your changes.

 Reflection identifies the macro as a "legacy macro," even though it's in a Reflection session document.

Editing Reflection Basic Macros

To edit Reflection Basic scripts

1 Open the Reflection Basic Editor.

2 Open the Reflection Basic script that you want to edit.

3 Use Application for the Reflection object name.

```
Code sample
```

4 (Optional) To access information or procedures in other Reflection Basic scripts, use the $Include metacommand, the Declare statement, or the RunScript method.

```
Code sample
```

To edit a Reflection Basic macro (script):

1 Open the Reflection Basic Editor.

2 Open the Reflection Basic script that you want to edit.

3 Optional: To access information or procedures in other Reflection Basic scripts, use the $Include metacommand, the RunScript method, or the Declare statement.

Example of the $Include metacommand:

This line of code, (the comment is intended) will make functions in the `common.rbs` available to the `.rbs` file.

'$include ".\common.rbs"

Example of the RunScript method:

This line of code runs the myTestRBScript.rbs script.

```
Application.RunScript "myTestRBScript.rbs", ""
```

Related Topics

◆

Run External Legacy Reflection Macro Dialog Box

Getting there

1 Open the Run Macro dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Reflection Ribbon	On the **Session**ribbon, from the **Macros**group, click **Run Macro**.
Reflection Browser	On the **Reflection** menu, choose **Tools**, **Macro**and then **Run Macro**.
TouchUx	Tap the Wrench icon and then under **Macro**, select **Show Run Macro Dialog**.

2 From the **Run Macro** dialog box, click **Legacy Reflection Macro in Another File**.

From this dialog box, you can run legacy Reflection macros (.rma, .rsf, .r2w, .r4w).

Settings or macro filename	Type the filename for the macro or click **Browse** to select it.
Select a macro	From the list, select the macro you want to run.
Macro data	Enter any parameters that you want to execute with the macro.

Run Embedded Macro with Data Dialog Box

Getting there

This dialog box opens when you initiate the action **Run Embedded Macro with Data**. To initiate an action, you must create a custom control, and then map an action to it. When you use the control, the action occurs.

1 Create a control using any of the following features:

- UI Designer

- per

- Mouse Mapper

- Context Menu Editor

2 From the **Select Action** dialog box, under **Action Category**, select **Macro**.

3 From the **Action** list, select **Run Embedded Macro with Data**, and then click **OK**.

The action is mapped to the control that you created in step 1.

4 Use the control to execute the **Run Embedded Macro with Data** action.

From this dialog box, you can run embedded legacy Reflection macros in open session documents.

Select Macro	From the list, specify the legacy Reflection macro that you want to run.
Macro Data	Enter any parameters that you want to execute with the selected macro.

Run Script Dialog Box

Getting there

1 Open the Run Macro dialog box.

The steps depend on your .

User Interface Mode	Steps
Reflection Ribbon	On the **Session**ribbon, from the **Macros**group, click **Run Macro**.
Reflection Browser	On the **Reflection** menu, choose **Tools**, **Macro**and then **Run Macro**.
TouchUx	Tap the Wrench icon and then under **Macro**, select **Show Run Macro Dialog**.

2 From the **Run Macro** dialog box, click **Legacy RB Macro**.

The options are:

File name	Specify the Reflection Basic macro file (.rbs) that you want by selecting it from the list, typing the name in the box, or browsing to select it.
Files of type	The default extension is .rbs. Reflection appends the extension .rbs to the filename.
Script arguments	Enter any arguments that you want to execute in the script.
Run	Choose to run the selected macro.

Extra! Macros

You can run most Extra! macro files (.ebm) in Reflection, including encrypted Extra! macros.

NOTE: To use Extra! macros in Reflection, you must install the Extra! feature when you install Reflection. (This feature is available on the Reflection Setup program Features tab, under **3270/5250 | Compatibility or UNIX and OpenVMS | Compatibility**.)

To run an Extra! macro

1 Open the Run Macro dialog box.

    1a The steps depend on your .

User Interface Mode	Steps
Reflection Ribbon	On the **Macros** tab, from the **Advanced** group, click **Run Macro**.
Reflection Browser	On the **Reflection** menu, choose **Tools**, **Macro** and then **Run Macro**.
TouchUx	Tap the Wrench icon and then under **Macro**, select **Show Run Macro Dialog**.

2 In the **Run Macro** dialog box, click **Extra! Macro**.

3 Browse to select a macro file, and then click **Open**. The macro must be in a trusted location.

NOTE

- If the macro contains unsupported objects, its functionality may be limited or it may not run.

- For a list of unsupported objects and methods, see the Reflection VBA Guide (**Help** > **VBA Guide**).

- Note: You can significantly improve the performance of your recorded Extra! macros by editing these macros to change how Reflection detects when the screen is ready for input. (See Knowledge Base Article 7021465 (https://support.microfocus.com/kb/doc.php?id=7021465).)

Video

▶◀ Running Extra! Macros Reflection Desktop (3:06)

Editing Extra! Macros

If you need to make changes to your Extra! macros (.ebm), you can edit them using the Extra! Basic Editor.

To start the Extra! Basic Editor, you must first associate the Run Extra! Basic Editor action with a custom control, such as a button or a keyboard shortcut.

NOTE: You can significantly improve the performance of your recorded Extra! macros by editing these macros to change how Reflection detects when the screen is ready for input.

For more information about how to run Extra! macros, set up the Basic editor, edit HostOptions properties, and improve performance of recorded macros, see Knowledge Base Article 7021465 (https://support.microfocus.com/kb/doc.php?id=7021465).

Related Topics

◆ "Select Action Dialog Box" on page 253

Rumba Macros

Reflection includes support for Micro Focus Rumba macros (.rmc).

NOTE: To run a Rumba macro, the Micro Focus Rumba compatibility feature must be installed. (This feature is installed by default.) It is available on the Reflection Setup program Features tab, under 3270/5250 | Compatibility.

To run a Rumba macro

1 Open the Run Macro dialog box.

    1a The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Reflection Ribbon	On the **Macros** tab, from the **Advanced** group, click **Run Macro**.
Reflection Browser	On the **Reflection** menu, choose **Tools**, **Macro** and then **Run Macro**.
TouchUx	Tap the Wrench icon and then under **Macro**, select **Show Run Macro Dialog**.

2 In the **Run Macro** dialog box, click **Rumba Macro**.

3 Browse to select a macro file, and then click **Open**.

IBM Personal Communications Macros

Reflection includes support for IBM Personal Communications macros (`.mac`).

NOTE: To run a Personal Communications macro, the IBM Personal Communications compatibility feature must be installed. This feature is available on the Reflection Setup program Features tab, under 3270/5250 | Compatibility.

To run a Personal Communications macro

1 Open the Run Macro dialog box.

    1a The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Reflection Ribbon	On the **Macros** tab, from the **Advanced** group, click **Run Macro**.
Reflection Browser	On the **Reflection** menu, choose **Tools**, **Macro** and then **Run Macro**.
TouchUx	Tap the Wrench icon and then under **Macro**, select **Show Run Macro Dialog**.

2 In the **Run Macro** dialog box, click **IBM Personal Communications Macro**.

3 Browse to select a macro file, and then click **Open**.

Brandon Systems\Jolly Giant QWS3270 Macros

Reflection supports QWS (.jgs) macros that run against IBM 3270 terminal sessions.

NOTE: To run a QWS macro, the Brandon Systems\Jolly Giant QWS3270 QWS compatibility feature must be installed. This feature is available on the Reflection Setup program Features tab, under 3270/5250 | Compatibility.

To run a QWS macro

1 Open the Run Macro dialog box.

    1a The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Reflection Ribbon	On the **Macros** tab, from the **Advanced** group, click **Run Macro**.
Reflection Browser	On the **Reflection** menu, choose **Tools**, **Macro** and then **Run Macro**.
TouchUx	Tap the Wrench icon and then under **Macro**, select **Show Run Macro Dialog**.

2 In the **Run Macro** dialog box, click **QWS Macro**.

3 Browse to select a macro file, and then click **Open**.

Hummingbird Basic Macros

Reflection supports OpenText HostExplorer Hummingbird Basic (.ebs) macros that run against IBM 3270 terminal sessions.

NOTE: To run a Hummingbird Basic macro, the HostExplorer compatibility feature must be installed. This feature is available on the Reflection Setup program Features tab, under 3270/5250 | Compatibility.

To run a Host Explorer macro

1 Open the Run Macro dialog box.

   1a The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Reflection Ribbon	On the **Macros** tab, from the **Advanced** group, click **Run Macro**.
Reflection Browser	On the **Reflection** menu, choose **Tools**, **Macro** and then **Run Macro**.
TouchUx	Tap the Wrench icon and then under **Macro**, select **Show Run Macro Dialog**.

2 In the **Run Macro** dialog box, click **HostExplorer Macro**.

3 Browse to select a macro file, and then click **Open**.

9 File and Data Transfer

Reflection supports the following methods for transferring information between your Windows computer and a host computer:

For IBM hosts:

- Mainframe file transfer is supported in 3270 sessions.
- IBM System i data transfer is supported in 5250 sessions. Other versions (including IBM AS/400, AS400, and iSeries systems) are also supported.
- FTP file transfer is supported in both 3270 and 5250 sessions.

For VT hosts:

- A Reflection proprietary protocol, which you can use to transfer files between your PC and an HP 3000 (including Classic, MPE/iX, and POSIX), VMS (including OpenVMS and Alpha computers), ULTRIX, Unisys, Linux Console or UNIX system.
- A variety of public domain protocols, including FTP.

Reflection also includes a separate, fully featured FTP client application available from any host session or from the Windows Start menu.

In this Chapter

IBM File and Data Transfer

Reflection supports the following methods for transferring information between your Windows computer and a host computer:

- Mainframe file transfer is supported in 3270 sessions.
- IBM System i data transfer is supported in 5250 sessions. Other versions (including IBM AS/400, AS400, and iSeries systems) are also supported.
- FTP file transfer is supported in both 3270 and 5250 sessions.

Mainframe File Transfer

From the **Transfer Settings** dialog box, you can configure global transfer setup for the current session document. Any configuration you perform is saved with your session document.

From the **Transfer** dialog box, you can configure and perform specific transfers. In 3270 sessions, you must be connected to a host to open the **Transfer** dialog box. If you frequently repeat the same transfers, use transfer request files to save specific transfer information, including which files to transfer.

NOTE: Reflection uses the IND$FILE host program by default for mainframe transfers, except on double-byte systems, when "APVUFILE" on page 897 is used.

Related Topics

- "Send Files to a Mainframe" on page 670
- "Receive Files from a Mainframe" on page 672
- "Mainframe Transfer Method Options" on page 673
- "Transfer Settings Dialog Box" on page 685
- "Transfer Request Files" on page 717
- "Batch Transfers" on page 719
- "Use File Transfer Naming Templates" on page 674

Send Files to a Mainframe

NOTE: If the transfer is one you'll be performing regularly, you can save your transfer settings in a transfer request file.

To transfer files to a mainframe from your PC

1 Connect and log on to the mainframe.

   The **File Transfer** button on the ribbon (or the **Transfer File** menu item if you are using Classic interface mode) is available only after you connect.

2 Open the File Transfer dialog box.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
The Reflection Ribbon	On the **Session** tab, from the **Transfer** group, click ⬆⬇ **File Transfer**.
Classic or Classic MDI	On the Tools menu, choose **Transfer File**.
The Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**.

3 Click the **Settings** button, and configure the file transfer settings.

For most situations, you can configure for file transfers by selecting a preset configuration in the **Protocol** tab.

4 Click **OK**.

5 From the **Transfer** dialog box, under **Local,** do one of the following:

- ◆ Browse under **Local folders**, and then select one or more files from the list.

  -or-

- ◆ Type the path and filename into the **File names** box.

6 Select your preferences for **Transfer method**, **If file exists**, and **Record format**.

7 Specify the host file information:

For this host system	Do this
CICS	Type a filename in the **File names** box.
	It is not possible to perform transfers involving multiple files.
	If you don't type a filename, Reflection uses the PC filename, with the period and extension, if applicable, removed. To avoid overwriting files, do not send files with the same filename and different extensions.
CMS	Click **Show host files**, and browse to select one or more host files.
	-or-
	Type the file information into the **File names** box.
	If you don't type a filename, Reflection uses the PC filename. If a PC file you are transferring does not have a file extension, the transfer fails.
TSO	Click **Show host files**, and browse to select one or more host files.
	All datasets that have a high-level qualifier that equals your user ID are displayed.
	-or-
	Type the file information into the **File names** box.
	If you don't type a filename, Reflection uses the PC filename.

8 To initiate a file transfer, do one of the following:

- ◆ Click the ⬚⬚ **Transfer** button.

  -or-

- ◆ Drag the source file, and then drop it on the desired destination file.

Related Topics

- ◆ "Receive Files from a Mainframe" on page 672
- ◆ "Mainframe Transfer Method Options" on page 673
- ◆ "Use File Transfer Naming Templates" on page 674

Receive Files from a Mainframe

NOTE: If the transfer is one you'll be performing regularly, you can save your transfer settings in a transfer request file.

To transfer files from a mainframe to the PC

1 Connect and log on to the mainframe.

   The **File Transfer** button on the ribbon (or the **Transfer File** menu item if you are using Classic interface mode) is available only after you connect.

2 Open the File Transfer dialog box.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
The Reflection Ribbon	On the **Session** tab, from the **Transfer** group, click ⬇ **File Transfer**.
Classic or Classic MDI	On the Tools menu, choose **Transfer File**.
The Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**.

3 Click the **Settings** button, and configure the file transfer settings.

   For most situations, you can configure for file transfers by selecting a preset configuration in the **Protocol** tab.

4 Click **OK**.

5 Specify a host file:

For this host system	Do this
CICS	Type a filename in the **File names** box.
	It is not possible to perform transfers involving multiple files.
CMS	Click **Show host files**, and browse to select one or more host files.
	To filter the list, you can enter partial filenames or wildcards; for example, to see all files that begin with the letter "d" of the mode "files" on the "a" disk, type the following:
	`d* files a`
	-or-
	Type the file information into the **File names** box.

For this host system	Do this
TSO	Click **Show host files**, and browse to select one or more host files.
	All datasets that have a high-level qualifier that equals your user ID are displayed.
	-or-
	Type the file information into the **File names** box.

6 Select your preferences for **Transfer method**, **If file exists**, and **Record format**.

7 From the **Transfer** dialog box, under **Local,** do one of the following:

   ◆ Browse under **Local folders**, and then select one or more files from the list.

     -or-

   ◆ Type the path and filename into the **File names** box.

   If you omit this step, Reflection uses the host filename.

8 To initiate a file transfer, do one of the following:

   ◆ Click the ⬛ **Transfer** button.

     -or-

   ◆ Drag the source file, and then drop it on the desired destination file.

Related Topics

   ◆ "Send Files to a Mainframe" on page 670

   ◆ "Mainframe Transfer Method Options" on page 673

   ◆ "Use File Transfer Naming Templates" on page 674

   ◆ "Transfer Dialog Box" on page 715

   ◆ "Transfer Settings Dialog Box" on page 685

   ◆ "Mainframe File Transfer" on page 670

Mainframe Transfer Method Options

Use the **Transfer method** setting in the **Transfer** dialog box to specify how files are converted. The options available depend on the file transfer protocol you have selected. For mainframe transfers the options are:

Binary	Use for program files and other types of files that should not be translated, such as files that have already been formatted for a particular type of printer or files with application-specific formatting. Binary files contain non-printable characters; using this method, a file is not converted or translated during the transfer.
ASCII	Use to transfer text files with no special formatting.
	ASCII files on the PC are translated to the EBCDIC character set on the host.
JISCII	Use for files that contain any double-byte characters with no special formatting. JISCII files are translated to the double-byte IBM host character set during transfer to the host.

Related Topics

- "Send Files to a Mainframe" on page 670
- "Receive Files from a Mainframe" on page 672
- "Transfer Dialog Box" on page 715
- "Mainframe File Transfer" on page 670
- "Configure File Transfer" on page 684
- "Saving and Repeating Transfers" on page 717
- "Batch Transfers" on page 719
- "Create a File Transfer Template" on page 675
- "Transfer Request Files" on page 717
- "Use File Transfer Naming Templates" on page 674

Use File Transfer Naming Templates

A file transfer template defines a set of conditions that affects how Reflection names files transferred between your PC and a host. Whereas transfer request files are used to transfer the same file or set of files between your PC and a host, file transfer templates affect how files transferred between your PC and a host are named.

When activated, Reflection checks transfer templates in the specified order, and tries to match the transferring filename to template conditions. When a match is found, the matching template is applied.

Reflection installs some default templates, but you can also add your own, and specify the sort order (using the **Move up** and **Move down** buttons).

To activate file transfer templates

1 Connect and log on to the mainframe.

The **File Transfer** button on the ribbon (or the **Transfer File** menu item if you are using Classic interface mode) is available only after you connect.

2 Open the Transfer Settings Dialog Box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Session** ribbon, from the **Transfer** group, click the **Transfer Settings** launcher:
Classic or Classic MDI	On the Tools menu, choose **Transfer File**. Then, in the Transfer dialog box, click the **Settings** button.
Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**. In the Transfer dialog box, click the **Settings** button.

3 On the **Protocol** tab, select **Mainframe** and then select the **Templates** tab.

4 Select **Activate transfer templates**.

5 Click **OK**.

Related Topics

- "Default File Transfer Templates" on page 677
- "Template Properties Dialog Box" on page 696
- "File Transfer Template Syntax" on page 678
- "Create a File Transfer Template" on page 675
- "Translation Tab (Transfer Settings Dialog Box)" on page 692
- "Transfer Request Files" on page 717
- "Mainframe File Transfer" on page 670

Create a File Transfer Template

Reflection installs some default templates, but you can also add your own, and specify the sort order (using the **Move up** and **Move down** buttons).

To create a file transfer template

1 Connect and log on to the mainframe.

2 Open the Transfer Settings Dialog Box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Session** ribbon, from the **Transfer** group, click the **Transfer Settings** launcher:
Classic or Classic MDI	On the Tools menu, choose **Transfer File**. Then, in the Transfer dialog box, click the **Settings** button.
Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**. In the Transfer dialog box, click the **Settings** button.

3 On the **Protocol** tab, select **Mainframe** and then select the **Templates** tab.

4 Select **Activate transfer templates**.

5 Click **New**.

6 From the **New Transfer Template** dialog box, type a PC filename condition and a host filename condition, using file transfer template syntax.

7 Select your preferences for **Transfer method**, **If file exists**, and **Record format**.

8 (Optional) To test your new template, click the **Test** button.

9 Click **OK**.

Related Topics

Test a File Transfer Template

You can access the **Test Template** dialog box from the **New Transfer Template** dialog box, or from the **Templates** tab of the **Transfer Settings** dialog box (with a template selected).

To test a file transfer template

1 Connect and log on to the mainframe.

2 Open the Transfer Settings Dialog Box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Session** ribbon, from the **Transfer** group, click the **Transfer Settings** launcher:
Classic or Classic MDI	On the Tools menu, choose **Transfer** File. Then, in the Transfer dialog box, click the **Settings** button.
Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**. In the Transfer dialog box, click the **Settings** button.

3 On the **Protocol** tab, select **Mainframe** and then select the **Templates** tab.

4 Select **Activate Transfer Templates**.

5 From the **Templates** list, select a template.

6 Click the **Test** button.

7 Type either a PC filename or a host filename to test.

8 Click one of the directional **Test** buttons to see how the filename will be affected by the transfer.

9 (Optional) To test your filename against all of the templates for a given host type, select **Test all templates**, select a host type, and then click one of the **Test** buttons.

Related Topics

Default File Transfer Templates

Reflection installs some default templates, but you can also add your own, and specify the sort order (using the **Move up** and **Move down** buttons).

Templates

CMS, ***.exe**, *** exebin a**
- All PC files with the .exe extension transferred to the host are given the extension "exebin" and stored on the A disk (the base name remains unchanged). For example, R8win.exe on the PC becomes R8win exebin on the host.
- All host files on the A disk with the extension "exebin" transferred to the PC are given the .exe extension (the base name remains unchanged). For example, R8win exebin becomes R8win.exe on the PC.

CMS, ***.txt**, *** text a**
- All PC files with the .txt extension transferred to the host are given the extension "text" and stored on the A disk (the base name remains unchanged). For example, Test.txt on the PC becomes Test text on the host.
- All host files on the A disk with the extension "text" transferred to the PC are given the .txt extension (the base name remains unchanged). For example, Test text becomes Test.txt on the PC.

CMS, ***.***, *** * a**
- All host files transferred to the PC keep their base name and extension (with a dot added) and are transferred from the A disk on the host. For example, Test text becomes Test.text.

  This condition is valid only for files transferred from a host.

TSO, ***.exe**, **bin.***
- All PC files with the .exe extension transferred to the host are prefixed with "bin." on the host (the base name remains unchanged). For example, Test.exe on the PC becomes Bin.test on the host.
- All host files prefixed with "bin." transferred to the PC are given the extension ".exe" (the base name remains unchanged). For example, Bin.test becomes Test.exe on the PC.

TSO, ***.txt**, **text.***	◆ All PC files with the .txt extension transferred to the host are prefixed with "text." on the host (the base name remains unchanged). For example, Filename.txt on the PC becomes Text.filename on the host.
	◆ All host files prefixed with "text." transferred to the PC are given the extension ".txt" (the base name remains unchanged). For example, Text.filename becomes Filename.txt on the PC.
CICS, ***.***, *****	◆ All PC files transferred to the host are stripped of their extension and retain just their base name. For example, Test.txt on the PC becomes Test on the host.
	◆ All host files transferred to the PC are given a dot extension (the base name remains unchanged). For example Test becomes Test. on the PC.

Related Topics

- ◆ "File Transfer Template Syntax" on page 678
- ◆ "Create a File Transfer Template" on page 675
- ◆ "Use File Transfer Naming Templates" on page 674
- ◆ "Templates Tab (Transfer Settings Dialog Box)" on page 693
- ◆ "Mainframe File Transfer" on page 670

File Transfer Template Syntax

Use the following syntax to create conditions for file transfer templates:

* (asterisk)	This works like a standard PC wildcard for one or more filename characters.
. (dot)	As in standard PC file naming, use to separate filenames from extensions.
=	Use in conjunction with the asterisk and the numerals 1-9 to identify the part of a filename you want to keep or strip out when transferring it.
	For example, if a host filename has three parts, such as `1.2.3`, and you want to keep just the second and third components of the filename when transferring it to your PC, you would use this condition:
	`*=1.*=2.*=3` (host file) ---> `*=2.*=3` (PC file)
`1-9`	Use the numerals 1 through 9 in conjunction with the asterisk (*) and the equal sign (=) to identify the part of a filename you want to keep or strip out when transferring it.
	For example, if a host filename has three parts, such as `Test.Text.Demo`, and you want to keep just the second and third components of the file name when transferring it to your PC, you would use this condition:
	`*=1.*=2.*=3` (host file) ---> `*=2.*=3` (PC file)
	which in this example would yield `Text.Demo`.

If a host filename has six parts and you want to keep the second and fifth parts when transferring it to your PC, the condition would be:

```
*=1.*=2.*=3.*=4.*=5.*=6 ---> *=2.*=5
```

You can use up to eight numerals in a condition.

Related Topics

- ◆ "New Transfer Template Dialog Box" on page 694
- ◆ "Create a File Transfer Template" on page 675
- ◆ "Use File Transfer Naming Templates" on page 674
- ◆ "Default File Transfer Templates" on page 677
- ◆ "Mainframe File Transfer" on page 670

Send.exe and Receive.exe

Reflection provides two command line utilities, Send.exe and Receive.exe, with which you can perform mainframe file transfers from a DOS command line prompt.

Send.exe

Use Send.exe to send a file to your mainframe host from a DOS prompt. The syntax for Send.exe is identical to the syntax of the HLLAPI function Send File (90).

Before sending a file, you must be connected to the host and at a ready prompt.

To send a file to the host using Send.exe, type the following from the DOS prompt:

```
send
     pc_filename
     PresentationSpace_shortname:
     host_filename [IND$FILE options]
```

Receive.exe

Use Receive.exe to receive a file from your mainframe host from a DOS prompt. The syntax for Receive.exe is identical to the syntax of the HLLAPI function Receive File (91).

Before receiving a file you must be connected to the host and at a ready prompt.

To receive a file from the host using Receive.exe, type the following from the DOS prompt:

```
receive
     pc_filename
     PresentationSpace_shortname:
     host_filename [IND$FILE options]
```

Related Topics

- ◆ "Send Files to a Mainframe" on page 670
- ◆ "Receive Files from a Mainframe" on page 672
- ◆ "Mainframe File Transfer" on page 670

DBCS File Transfer Settings

The following table shows the effects that the DBCS file transfer settings NOSO, SO, and User Mode have on the characters SO (hex 0E), SI (hex 0F), RS (hex 1E) and US (hex 1F) when they appear in files sent to or received from the host.

NOSO (Sending)	SO (Receiving)	User Mode (Receiving)	Effects on File
Selected	n/a	n/a	RS/US (hex 1E and hex 1F) characters are removed when the PC file is sent to the host.
			SO/SI (hex 0E and hex 0F) characters are not sent to the host when a transition to or from single-byte to double-byte format is detected.
Cleared	n/a	n/a	RS/US (hex 1E and hex 1F) characters are converted to SO/SI (hex 0E and hex 0F), respectively when the file is sent to the host.
			SO/SI (hex 0E and hex 0F) characters are converted to NUL when the file is sent to the host.
			Note: This character translation can be edited using the 3270 Single-byte Translation Table Editor (Edit3270.exe).
n/a	Selected	Cleared	SO/SI (hex 0E and hex 0F) characters are converted to RS/US (hex 1E and hex 1F), respectively, when the host file is received.
n/a	Selected	Selected	SO/SI (hex 0E and hex 0F) characters are kept intact when the host file is received.
n/a	Cleared	Cleared	The host file is received from the host as is, with no changes.
n/a	Cleared	Selected	The host file is received from the host as is, with no changes.

Related Topics

- "CMS Advanced Options Dialog Box" on page 688
- "TSO Advanced Options Dialog Box" on page 689
- "CICS Advanced Options Dialog Box" on page 691

IBM System i (AS/400) Transfer

From the **Transfer Settings** dialog box, you can configure global transfer settings for the current session document. For IBM System i (AS/400) transfer, Reflection creates a new connection to the host. If you don't want to be prompted each time you transfer files, you can save your user name and password information on the **AS/400** tab. Any configuration you perform is saved with your session document.

From the **Transfer** dialog box, you can configure and perform specific transfers. In 5250 sessions you don't need to be connected to a host to open this dialog box. If you frequently repeat the same transfers, use transfer request files to save specific transfer information, including which files to transfer.

A common way to receive data from an IBM System i host is to collect only the data you need from one or more files in the host database. To do this you can create an SQL query. Query information can also be saved to a transfer request file.

Related Topics

- "Transfer Data to or From an IBM System i (AS/400)" on page 126
- "IBM System i (AS/400) Field Description Files" on page 681
- "Create an SQL Query" on page 682
- "Transfer Request Files" on page 717
- "Batch Transfers" on page 719
- "IBM System i (AS/400) Transfer Method Options" on page 683
- "Configure File Transfer" on page 684
- "Saving and Repeating Transfers" on page 717

IBM System i (AS/400) Field Description Files

A description file is a text file in ASCII format that contains descriptions of each field in a corresponding data file, which allows you to keep data in the intended format when sending data to the host. Field description files are created by default during data transfers to your PC.

The description file has the same name as the data file, except for the extension, which is `.FDF`. You'll see its name in the **Local file names** box in the **Transfer** dialog box.

If the file you're sending did not originate on the host, and has never been transferred to the host, you must create a description file before you can send a PC file to the host.

Your system administrator may have created a generic description file that resides on the host and can be downloaded, modified, and saved with a new name. (Check with your system administrator to see if this option is available.) Or, you can create your own description file. Refer to your IBM System i (AS/400) documentation for more information.

Related Topics

- "Drag-and-Drop Options for Receiving from an IBM System i (AS/400)" on page 682
- "Create an SQL Query" on page 682
- "IBM System i (AS/400) Transfer Method Options" on page 683
- "IBM System i (AS/400) Field Description Files" on page 681
- "Transfer Data to or From an IBM System i (AS/400)" on page 126
- "IBM System i (AS/400) Transfer" on page 681

Drag-and-Drop Options for Receiving from an IBM System i (AS/400)

From the **Transfer** dialog box, you can drag IBM System i (AS/400) host files to a listed PC file or to an item in **Local folders**. (First, make sure that the value for the **If File Exists** is appropriate.)

Following are the possible scenarios:

- Host file to **Local folders** box

The first member of the selected host file is copied to the local folder on which it is dropped.

- ◆ Host file to PC file

  The first member of the selected host file is copied to the PC file on which it was dropped.

- ◆ Host member to **Local folders** box

  The selected member is copied to the folder on which it was dropped.

- ◆ Host member to PC file

  The selected member is copied to the selected PC file.

Related Topics

- ◆ "Transfer Data to or From an IBM System i (AS/400)" on page 126
- ◆ "IBM System i (AS/400) Transfer" on page 681

Create an SQL Query

A common way to receive data from an IBM System i (AS/400) is to collect only the data you need from one or more files in the host database; for example, to assemble a list of employee addresses and payroll information, you can collect and transfer only that information to a PC file or to your display, even if the information resides in different host files. You can also specify how to sort data or set conditions that determine which records are transferred. To do this, you would create an SQL query.

If you need help building your SQL query, consult your SQL documentation.

To create an SQL query

1 Open the File Transfer dialog box.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
The Reflection Ribbon	On the **Session** tab, from the **Transfer** group, click **File Transfer**.
Classic or Classic MDI	On the Tools menu, choose **Transfer File**.
The Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**.

2 Click **Show Host Files**. (It may be necessary to enter your user name and password.)

3 Select one or more host files from which to transfer data.

4 Click **Settings**, and then click the **SQL** tab.

   The database options **Select**, **Where**, **Order by**, **Group by**, **Having**, and **Join by** appear as text boxes.

5 Do one of the following:

- ◆ If you already know the syntax for the statement or clause, type it in the text box.

  -or-

- ◆ If you don't know how to create the statement or clause, click the arrow button to the right of the option, and then in the dialog box that opens, specify the field names, functions, operators, options and so on.

The statement is automatically created from your selections.

> **NOTE:** If the transfer is one you'll be performing regularly, you can save your transfer settings in a transfer request file.

Related Topics

IBM System i (AS/400) Transfer Method Options

Use the **Transfer method** setting in the **Transfer** dialog box to specify how data in files is processed during transfers.

> **NOTE:** This setting does not affect transfers to the host when you are using a description file to keep data in the intended format. Reflection uses description files by default. You can change this configuration from the **Options** tab of the **Transfer Settings** dialog box.

The options available depend on the file transfer protocol you have selected. For IBM System i (AS/400) transfers, the options are:

ASCII	Use for files with no special formatting, and fixed record widths.
Basic Sequential	Use to separate all fields with commas, and insert quotation marks around character and hexadecimal fields.
BIFF	Use for files transferred to and from Microsoft Excel and other spreadsheet applications. This includes binary file formats used by Microsoft Excel, prior to the BIFF8 version.
	You can select whether to include field names in the data transfer.
BIFF8	Use for files transferred to and from Microsoft Excel and other spreadsheet applications. This is the binary file format used by Microsoft Excel, versions 97-2003 (.xls). No more than 65536 rows are allowed.
	You can select whether to include field names in the data transfer.
CSV	Use to separate fields with commas, and insert quotation marks only around character fields that contain a comma or quotation mark.
DIF	Use for files transferred to and from Microsoft Excel and other spreadsheet applications — Data Interchange Format (DIF) files contain the field names. This format does not support multiple spreadsheets.
DOS Random	Use for data transferred to and from the host from host database applications that require data to be in DOS Random format.
No Conversion	Use for files that should not be translated — files transferred as No Conversion are not translated to the EBCDIC character set during a transfer to the host.
Tab Delimited	Use to separate all fields with tabs, and insert quotation marks only around character fields that contain a quotation mark.

Related Topics

Configure File Transfer

You can manually configure file transfer settings in the **Transfer Settings** dialog box. Any configuration you perform is saved with your session document.

However, using the automated preset configurations is recommended.

To configure file transfer

1 Open the File Transfer dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
The Reflection Ribbon	On the **Session** tab, from the **Transfer** group, click **File Transfer**.
Classic or Classic MDI	On the Tools menu, choose **Transfer File**.
The Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**.

2 Click the **Settings** button, and configure the file transfer settings.

For most situations, you can configure for file transfers by selecting a preset configuration in the **Protocol** tab.

Related Topics

- "Transfer Settings Dialog Box" on page 685

Transfer Settings Dialog Box

Getting there

1 Open the Transfer Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Session** ribbon, from the **Transfer** group, click the **Transfer Settings** launcher:
Classic or Classic MDI	On the Tools menu, choose **Transfer** File. Then, in the Transfer dialog box, click the **Settings** button.
Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**. In the Transfer dialog box, click the **Settings** button.

Configure transfer protocol and translation options for file and data transfers. Any configuration you perform is saved with your session document. The tabs displayed depend on your current configuration, and the way you accessed this dialog box.

Protocol (page 686)

Available in all session types. Use this tab to select a transfer protocol.

Mainframe (page 687)

Available in 3270 sessions when Mainframe is the selected protocol. Use this tab to configure transfer protocol options when you're transferring to or from an IBM mainframe.

Translation (page 692)

Available in all sessions when Mainframe or AS/400 is the selected protocol. Use this tab to specify how filenames are handled during transfers.

Templates (page 693)

Available in 3270 sessions when Mainframe is the selected protocol. Use this tab to map PC filename patterns to filename patterns on the mainframe.

AS/400 (page 698)

Available in all sessions when AS/400 is the selected protocol. Use this tab to configure transfer protocol connection options for transfers to and from an IBM System i (AS/400).

Options (page 702)

Available in all sessions when AS/400 is the selected protocol. Use this tab to configure the way Reflection handles data transfer.

SQL (page 704)

Available when AS/400 is the selected protocol, and you open the **Transfer Settings** dialog box by clicking the **Settings** button in the **Transfer** dialog box. Use this tab to create SQL queries for extracting data from IBM System i (AS/400) files.

FTP (page 713)

Available in both 3270 and 5250 sessions.

Related Topics

◆ "Batch Transfers" on page 719
◆ "Send Files to a Mainframe" on page 670

Protocol Tab (Transfer Settings Dialog Box)

Getting there

1 Open the Transfer Settings dialog box.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Session** ribbon, from the **Transfer** group, click the **Transfer Settings** launcher:
Classic or Classic MDI	On the Tools menu, choose **Transfer** File. Then, in the Transfer dialog box, click the **Settings** button.
Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**. In the Transfer dialog box, click the **Settings** button.

The protocol you select determines which preset configurations are available. Also, the tabs available from the **Transfer Settings** dialog box change to enable you to configure transfers using the selected protocol.

Protocol	Select the file transfer protocol you want to use.
Preset configurations	Selecting an item from this list adjusts the appropriate values automatically in the **Transfer Settings**dialog box for that specific environment.

Related Topics

◆ "Transfer Settings Dialog Box" on page 685

Mainframe Tab (Transfer Settings Dialog Box)

Getting there

1 Open a 3270 terminal session and then open the Transfer Settings dialog box.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Session** ribbon, from the **Transfer** group, click the **Transfer Settings** launcher:
Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**. In the Transfer dialog box, click the **Settings** button.
TouchUx	Tap the Wrench icon and then under **Tools**, select **File Transfer**. In the Transfer dialog box, click the **Settings** button.

2 With **Mainframe** selected under **Protocol**, click the **Mainframe** tab.

The options are:

Host

System	Select the operating system the host is running.
Startup command	Type the name of the host program to be issued by Reflection to initiate a file transfer. The default value, IND$FILE, is appropriate for CMS and TSO hosts.
	For CICS hosts, IND$FILE may be appropriate, or you may need to specify your site's CICS transaction (for example, CFTR).
	When working with double-byte characters, use “APVUFILE” on page 897.
Advanced	Configure advanced options for the selected host system type (CICS, CMS, or TSO).

Structured field transfer

Max field size	Select a buffer value (other than **Disabled**) to have Reflection use the **Write Structured Field** protocol. As a rule, the larger the buffer size, the faster the transfer. However, if you select a value that is too large for your host, it will disconnect your session when you first attempt to send a file big enough to fill the buffer.
	This option is relevant for IND$FILE, “APVUFILE” on page 897 and DISOSS transfers.

Timeout (in seconds)

Startup	Set the amount of time Reflection should wait for a host response when attempting to connect. Select a value between 1-9999.
Response	Set the amount of time Reflection should wait for a host response. Select a value between 1-9999.

Related Topics

-

CMS Advanced Options Dialog Box

Getting there

1 Open a 3270 terminal session and then open the Transfer Settings dialog box.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Session** ribbon, from the **Transfer** group, click the **Transfer Settings** launcher:
Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**. In the Transfer dialog box, click the **Settings** button.
TouchUx	Tap the Wrench icon and then under **Tools**, select **File Transfer**. In the Transfer dialog box, click the **Settings** button.

2 With **Mainframe** selected under **Protocol**, click the **Mainframe** tab.

3 Under **Host**, from the **System** list, select **CMS**.

4 Click the **Advanced** button.

The options are:

Logical record length	Type the record size (in bytes) for the file being created on the host. If you leave this box blank, the record size is determined by the host. Use a value between 0 and 32768 to accommodate the range accepted by your host. For ASCII files, set this value to accommodate the longest line in your file. When you leave this box blank, the host typically accepts lines of up to 80 characters.

CR/LF processing

When you select one of these options, a carriage return character and a linefeed character are stripped from the end of each line of the file you are sending.

CR/LF processing is typically appropriate for ASCII and JISCII files but not for binary files; the defaults for these options are set up accordingly.

Additional IND$FILE parameters	Use this text box for any parameters specific to the IND$FILE (or APVUFILE) program on your host system. The contents of this text box are appended to the end of the transfer command generated by Reflection. Reflection does not check the contents of this text box for validity.

For a description of the **NOSO**, **SO**, and **User Mode** settings, see the "DBCS File Transfer Settings" on page 680 topic.

Related Topics

◆ "DBCS File Transfer Settings" on page 680

◆ "Mainframe Tab (Transfer Settings Dialog Box)" on page 687

◆ "Mainframe File Transfer" on page 670

TSO Advanced Options Dialog Box

Getting there

1 Open a 3270 terminal session and then open the Transfer Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Session** ribbon, from the **Transfer** group, click the **Transfer Settings** launcher:
Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**. In the Transfer dialog box, click the **Settings** button.
TouchUx	Tap the Wrench icon and then under **Tools**, select **File Transfer**. In the Transfer dialog box, click the **Settings** button.

2 With **Mainframe** selected under **Protocol**, click the **Mainframe** tab.

3 Under **Host**, from the **System** list, select **TSO**.

4 Click the **Advanced** button.

The options are:

Dataset options

Logical record length	Type the record size (in bytes) for the file being created on the host. If you leave this box blank, the record size is determined by the host. Use a value between 0 and 32768 to accommodate the range accepted by your host.
	For ASCII files, set this value to accommodate the longest line in your file. When you leave this box blank, the host typically accepts lines of up to 80 characters.
Block size	Type the block size (in bytes) for the file being created on the host. For files with fixed-length records, this value must be a multiple of the **Logical record length** (because blocks are divided into logical records).
	Use a value between 0 and 32768 to accommodate the range accepted by your host.

Space allocation

Allocation units	Select the disk subdivisions for your primary and secondary space allocations. If you select **Default**, the unit is determined by the host. If you select **Block**, use the **Average block** box to set the size for an average block.
Average block	Type the size (in bytes) for an average block. This value is only relevant if you are using blocks as your allocation unit.
Primary	Type the size (in allocation units) of the primary allocation for the host file being created.
Secondary	Type the size of any additional allocations (in allocation units) in the event that the primary allocation is not sufficient. Multiple secondary allocations (known as "extents") are allowed, up to a host-specified limit (generally 15).

CR/LF processing

When you select one of these options, a carriage return character and a linefeed character are stripped from the end of each line of the file you are sending.

CR/LF processing is typically appropriate for ASCII and JISCII files but not for binary files; the defaults for these options are set up accordingly.

Additional IND$FILE parameters	Use this text box for any parameters specific to the IND$FILE (or APVUFILE) program on your host system. The contents of this text box are appended to the end of the transfer command generated by Reflection. Reflection does not check the contents of this text box for validity.

For a description of the **NOSO**, **SO**, and **User Mode** settings, see the "DBCS File Transfer Settings" on page 680 topic.

Related Topics

◆ "DBCS File Transfer Settings" on page 680

◆ "Mainframe Tab (Transfer Settings Dialog Box)" on page 687

◆ "Mainframe File Transfer" on page 670

CICS Advanced Options Dialog Box

Getting there

1 Open a 3270 terminal session and then open the Transfer Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Session** ribbon, from the **Transfer** group, click the **Transfer Settings** launcher:
Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**. In the Transfer dialog box, click the **Settings** button.
TouchUx	Tap the Wrench icon and then under **Tools**, select **File Transfer**. In the Transfer dialog box, click the **Settings** button.

2 With **Mainframe** selected under **Protocol**, click the **Mainframe** tab.

3 Under **Host**, from the **System** list, select **CICS**.

4 Click the **Advanced** button.

The options are:

CR/LF processing

When you select one of these options, a carriage return character and a linefeed character are stripped from the end of each line of the file you are sending.

CR/LF processing is typically appropriate for ASCII and JISCII files but not for binary files; the defaults for these options are set up accordingly.

Additional IND$FILE parameters	Use this text box for any parameters specific to the IND$FILE (or APVUFILE) program on your host system. The contents of this text box are appended to the end of the transfer command generated by Reflection. Reflection does not check the contents of this text box for validity.

For a description of the **NOSO**, **SO**, and **User Mode** settings, see the "DBCS File Transfer Settings" on page 680 topic.

Related Topics

◆ "DBCS File Transfer Settings" on page 680

◆ "Mainframe Tab (Transfer Settings Dialog Box)" on page 687

◆ "Mainframe File Transfer" on page 670

Translation Tab (Transfer Settings Dialog Box)

Getting there

1 Open the Transfer Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Session** ribbon, from the **Transfer** group, click the **Transfer Settings** launcher:
Classic or Classic MDI	On the Tools menu, choose **Transfer** File. Then, in the Transfer dialog box, click the **Settings** button.
Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**. In the Transfer dialog box, click the **Settings** button.

The options are:

Filename translation options

Change spaces to underscores when sending	Select to convert spaces in filenames to underscores in files sent to the host. If your host does not support spaces in filenames, this prevents the host from modifying the filename or rejecting the transfer.
Change underscores to spaces when receiving	Select to convert underscores in filenames to spaces in files received from the host.
	By selecting this option in conjunction with the **Change spaces to underscores when sending** option, you satisfy the conventions of both the PC and the host, yet maintain the appearance of an unchanged file name: The name change occurs, but is transparent to both the PC and the host.
Truncate received filenames to 8.3 format	Select to receive host files in the DOS 8.3 filename format.
	For example, a file with the name `Longfilename.Document` will be converted automatically to `Longfile.doc` when transferred to your PC.
Display 8.3 filenames as	Select how you want filenames conforming to the DOS 8.3 file naming convention to display under **Local** in the **Transfer** dialog box.

Related Topics

◆ "IBM File and Data Transfer" on page 669

Templates Tab (Transfer Settings Dialog Box)

Getting there

1 Open a 3270 terminal session and then open the Transfer Settings dialog box.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Session** ribbon, from the **Transfer** group, click the **Transfer Settings** launcher:
Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**. In the Transfer dialog box, click the **Settings** button.
TouchUx	Tap the Wrench icon and then under **Tools**, select **File Transfer**. In the Transfer dialog box, click the **Settings** button.

2 With **Mainframe** selected under **Protocol**, click the **Templates** tab.

File transfer templates are available when the transfer protocol is set to Mainframe. These templates define a set of conditions that affect the way Reflection names files transferred between your Windows computer and a host. Unlike transfer request files, which are used to transfer the same file or set of files between your computer and a host, file transfer templates affect the how all files transferred between your computer and the host are named. You can create multiple conditions for Reflection to step through until it finds the first one that is applicable.

With file transfer templates, for example, you can send all local files with the extension .EXE to the host, and give them the extension .EXEC.

Activate transfer templates	Select to enable file transfer templates for all files transferred to or received from the host. When selected, Reflection steps through the list of file transfer templates to find a matching condition each time you transfer a file to or from the host.
Templates	Lists the templates that have been defined.
New	Add a new template to the list.
Remove	Remove the selected template.
Properties	View and edit the properties of the selected template.
Test	Open the **Test Template** dialog box, from which you can test how Reflection handles sample filename conditions without actually having to transfer a file.
Move up	Move the selected item in the list.
Move down	Move the selected item in the list.

Related Topics

- "Default File Transfer Templates" on page 677
- "Use File Transfer Naming Templates" on page 674

New Transfer Template Dialog Box

Getting there

1 Open a 3270 terminal session.

2 Open the Transfer Settings Dialog Box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Session** ribbon, from the **Transfer** group, click the **Transfer Settings** launcher: 🖫
Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**. In the Transfer dialog box, click the **Settings** button.
TouchUx	Tap the Wrench icon and then under **Tools**, select **File Transfer**. In the Transfer dialog box, click the **Settings** button.

3 With **Mainframe** selected under **Protocol**, click the **Templates** tab.

4 Select **Activate Transfer Templates**.

5 Click **New**.

The options are:

PC file name	Type the PC filename parameters. This condition is used for files transferred to and from the host.
Host file name	Type the host filename parameters. This condition is used for files transferred to and from the host.
Host type	Select the operating system the host is running.
Transfer type	When you perform a file transfer, it defaults to the transfer type you select from this list.
If file exists	Select what to do when the transferred file already exists in the target location.
Record format	Select the record format to use for transfers to the host:

Select	To
Fixed	Force the host to create fixed-length records.

Undefined	Force the host to create files without a specific record format (this value is only relevant for TSO systems).
Variable	Force the host to create variable-length records and preserve the format of a binary file.
Default	Let the host determine the record format.
Advanced	Configure advanced options for the selected host system type (CICS, CMS, or TSO).
Test	Open the **Test Template** dialog box, from which you can test how Reflection handles sample filename conditions without actually having to transfer a file.

Related Topics

Template Properties Dialog Box

Getting there

1 Open a 3270 terminal session.

2 Open the Transfer Settings Dialog Box.

   The steps depend on your .

User Interface Mode	Steps
Ribbon	On the **Session** ribbon, from the **Transfer** group, click the **Transfer Settings** launcher:
Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**. In the Transfer dialog box, click the **Settings** button.
TouchUx	Tap the Wrench icon and then under **Tools**, select **File Transfer**. In the Transfer dialog box, click the **Settings** button.

3 With **Mainframe** selected under **Protocol**, click the **Templates** tab.

4 Select **Activate Transfer Templates**.

5 From the **Templates** list, select a template.

6 Click the **Properties** button.

The options are:

PC file name	Type the PC filename parameters. This condition is used for files transferred to and from the host.
Host file name	Type the host filename parameters. This condition is used for files transferred to and from the host.
Host type	Select the operating system the host is running.
Transfer type	When you perform a file transfer, it defaults to the transfer type you select from this list.
If file exists	Select what to do when the transferred file already exists in the target location.
Record format	Select the record format to use for transfers to the host:

Select	To
Fixed	Force the host to create fixed-length records.
Undefined	Force the host to create files without a specific record format (this value is only relevant for TSO systems).
Variable	Force the host to create variable-length records and preserve the format of a binary file.
Default	Let the host determine the record format.

Advanced	Configure advanced options for the selected host system type (CICS, CMS, or TSO).
Test	Open the **Test Template** dialog box, from which you can test how Reflection handles sample filename conditions without actually having to transfer a file.

Related Topics

Test Template Dialog Box

Getting there

1 Open a 3270 terminal session.

2 Open the Transfer Settings Dialog Box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Session** ribbon, from the **Transfer** group, click the **Transfer Settings** launcher:
Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**. In the Transfer dialog box, click the **Settings** button.
TouchUx	Tap the Wrench icon and then under **Tools**, select **File Transfer**. In the Transfer dialog box, click the **Settings** button.

3 With **Mainframe** selected under **Protocol**, click the **Templates** tab.

4 Select **Activate Transfer Templates**.

5 From the **Templates** list, select a template.

6 Click the **Test** button.

The options are:

PC file name	Type the PC filename parameters. This condition is used for files transferred to and from the host.
Host file name	Type the host filename parameters. This condition is used for files transferred to and from the host.
Test all templates	Select to perform a test using all the currently defined conditions for the selected host type. When more than one condition is defined, Reflection steps through them in the order they appear in the **Templates** list.
Host Type	Select the host type for which you want to test all templates.

Related Topics

- "Test a File Transfer Template" on page 676
- "File Transfer Template Syntax" on page 678
- "Create a File Transfer Template" on page 675
- "Use File Transfer Naming Templates" on page 674
- "Mainframe File Transfer" on page 670

AS/400 Tab (Transfer Settings Dialog Box)

Getting there

1 Open a 3270 or 5250 terminal session.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Session** ribbon, from the **Transfer** group, click the **Transfer Settings** launcher: ⬚
Reflection Browser	On the Reflection menu, choose **Tools**and then **File Transfer**. In the Transfer dialog box, click the **Settings**button.
TouchUx	Tap the Wrench icon and then under **Tools**, select **File Transfer**. In the Transfer dialog box, click the **Settings**button.

2 From the **Protocol** list, select **AS/400**.

3 Click the **AS/400**tab.

The options are:

Transport	TCP/IP is the only supported transfer type.
Host TP	Select an AS/400 data transfer transaction program to use. **LIPI** supports more complex SQL statements.
National character set	Select a character set to use for character translations during IBM System i (AS/400) data transfers.
PC characters	Select a character set. This option is relevant for data that contains characters with decimal values above 127. (ANSI and ASCII character sets have the same values for characters with decimal values from 32 – 126.)
System name	Type the host name to use for IBM System i (AS/400) data transfers. You can enter the name of the host your session is connected to or enter another host name.
Use Windows credentials	Use your Windows credentials instead of your IBM System i (AS/400) username and password to bypass being prompted when performing a data transfer.
Username	Enter the username you use to log on to the IBM System i (AS/400) to bypass being prompted for it before performing a data transfer.
Password	Enter the password you use to log on to the IBM System i (AS/400) to bypass being prompted for it before performing a data transfer.
Advanced	Configure advanced TCP/IP options.
Fields	Set format options for the database fields you receive from the host.
Security	Secure data communications with SOCKS or SSL/TLS.

Timeout (in seconds)

Startup	Set the amount of time Reflection should wait for a host response when attempting to connect. Select a value between 1-9999.
Response	Set the amount of time Reflection should wait for a host response. Select a value between 1-9999.

Related Topics

- "IBM System i (AS/400) Transfer" on page 681
- "Database Field Options Dialog Box" on page 700

Advanced TCP/IP Dialog Box

Getting there

1 Open a 3270 or 5250 terminal session.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Session** ribbon, from the **Transfer** group, click the **Transfer Settings** launcher:
Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**. In the Transfer dialog box, click the **Settings** button.
TouchUx	Tap the Wrench icon and then under **Tools**, select **File Transfer**. In the Transfer dialog box, click the **Settings** button.

2 From the **Protocol** list, select **AS/400**.

3 Click the **AS/400**tab.

4 Click the **Advanced** button.

The options are:

IP address	Type the host system address here if you do not have a Hosts file, and your system name does not have an IP address entry in the Domain Name Server for which your TCP/IP stack is configured.
Use default ports	Clear this check box to allow Reflection to communicate with host transaction programs using non-standard port numbers.

Related Topics

- "AS/400 Tab (Transfer Settings Dialog Box)" on page 698
- "IBM System i (AS/400) Transfer" on page 681

Database Field Options Dialog Box

Getting there

1 Open a 3270 or 5250 terminal session.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Session** ribbon, from the **Transfer** group, click the **Transfer Settings** launcher:
Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**. In the Transfer dialog box, click the **Settings** button.
TouchUx	Tap the Wrench icon and then under **Tools**, select **File Transfer**. In the Transfer dialog box, click the **Settings** button.

2 From the **Protocol** list, select **AS/400**.

3 Click the **AS/400**tab.

4 Click the **Fields** button.

Set format options for the database fields you receive from the host.

Time

Format	Select the time format for selected fields with an IBM System i (AS/400) field type of Time. The options are:	
	DDS	Format given by IBM System i (AS/400) file attribute.
	DFT	IBM System i (AS/400) job default (default).
	EUR	IBM European standard (hh.mm.ss).
	HMS	Hour, minute, second (hh:mm:ss).
	ISO	International Standards Organization (hh.mm.ss).
	JIS	Japanese Industrial Standard (hh:mm:ss).
	USA	USA standard (hh:mm AM or PM).
Separator	Select a character to use as a time separator in selected fields having an IBM System i (AS/400) field type of Time.	

Date

Format	Select the date format for selected fields having an IBM System i (AS/400) field type of Date. The options are:	
	DDS	Format given by IBM System i (AS/400) file attribute.
	DFT	IBM System i (AS/400) job default (default).

DMY	Day, month, year (dd/mm/yy)	
EUR	IBM European standard (dd.mm.yyyy).	
ISO	International Standards Organization (yyyy/mm/dd).	
JIS	Japanese Industrial Standard (yyyy-mm-dd).	
JULIAN	(yy/ddd)	
MDY	Month, day, year (mm/dd/yy).	
USA	USA standard (mm/dd/yyyy).	
YMD	Year, month, day (yy/mm/dd).	

Separator   Select a character to use as a date separator in selected fields having an IBM System i (AS/400) field type of Date.

Ignore decimal data errors   Select to ignore any decimal data errors found in a packed or zoned field during the transfer from the IBM System i (AS/400). Ignoring these errors speeds up the transfer process.

Decimal separator   Select the character to use as a decimal separator in selected fields that have an IBM System i (AS/400) field type of packed decimal or zoned decimal.

Sort sequence   Select a sort sequence for the data being transferred. This sequence determines the order of characters in the alphabet when fields are alphabetized. The sort sequence also affects any comparisons based on characters in the fields. The options are:

*HEX	Uses the EBCDIC hexadecimal sort sequence.
*JOB	Uses the IBM System i (AS/400) job default.
*LANGIDSHR	Uses a shared weight table.
*LANGIDUNQ	Uses a unique weight table.

Related Topics

 ◆ "AS/400 Tab (Transfer Settings Dialog Box)" on page 698

 ◆ "IBM System i (AS/400) Transfer" on page 681

Options Tab (Transfer Settings Dialog Box)

Getting there

1 Open a 5250 terminal session.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Session** ribbon, from the **Transfer** group, click the **Transfer Settings** launcher: ⬚
Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**. In the Transfer dialog box, click the **Settings** button.
TouchUx	Tap the Wrench icon and then under **Tools**, select **File Transfer**. In the Transfer dialog box, click the **Settings** button.

2 From the **Protocol** list, select **AS/400**.

3 Click the **Options** tab.

From host

Save description	Select to save description files associated with files you receive from the host. Description files are only relevant when you are receiving data output to a file, rather than to your display.
Description file	Type a description filename. By default, Reflection creates a description file that has the same name as its corresponding data file, but with an .FDF extension.
Show transfer progress	Select to display a progress bar during transfers from the host. Transfers take less time when this check box is cleared because the IBM System i (AS/400) does not have to count the number of selected records before transferring them.
Delete trailing spaces (ASCII only)	Select to remove extra spaces at the end of a record when the data is received.
Output to	Select where to direct received data. Use Display to display data in the Query Results window. Use Spreadsheet to save data to a .DIF, BIFF, or BIFF8 file.
Save column header (BIFF and BIFF8 only)	Select to include the field names as column headers in BIFF and BIFF8 transfers.

To host

Use description	Select to use description files with files you receive from the host.
Description file	Enter a description file path and file name. By default, Reflection creates a description file that has the same name as its corresponding data file, but with an .FDF extension.
Objects	Select whether data is transferred to a new or existing member on the IBM System i (AS/400).

Select	To
Create File And Member	Create a new member within a new host file. To use this option, specify a host library in the Transfer dialog box.

Create Member	Create a new member within an existing host file.
Replace Member (Confirm)	Send data to an existing member in an existing file and prompt for confirmation of the overwrite action.
Replace Member (Don't Confirm)	Send data to an existing member in an existing file without being prompted to confirm the overwrite action.

File type	If you are creating a file on the host, select the type of file to create.
	If you aren't using a description file, this setting will be determined by host defaults.
Authority	Set permissions for the new host file.
File text	Describe the new host file.
Member text	Describe the new member.
Record length	Select the record size (in bytes) for the new host file. This setting is unavailable if you are using a description file.
Reference file	Specify a reference file to use for the file you are sending. The new host file is created using the field names in the description file and the definitions of the fields in the reference file.
	The syntax for specifying a reference file is:
	library_name/filename
	NOTE: A reference file is a physical file that defines the fields used in other files. You can create a field reference file to contains only the field descriptions that you need for any group of files or you can specify a file that has the same fields as the file you are creating.

Related Topics

* "IBM System i (AS/400) Field Description Files" on page 681
* "IBM System i (AS/400) Transfer" on page 681

SQL Tab (Transfer Settings Dialog Box)

Getting there

1 Open the Transfer Dialog box.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
The Reflection Ribbon	On the **Session** tab, from the **Transfer** group, click **File Transfer**.
The Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**.
TouchUx	Tap the Wrench icon and then under **Tools**, select **File Transfer**.

2 If you are running a 3270 session, change the protocol to AS/400.

    2a Click **Settings**.

    2b From the **Protocol** list, select **AS/400**.

    2c Click **OK**.

3 Click **Show Host Files**. (It may be necessary to enter your user name and password.)

4 Select one or more host files from which to transfer data.

5 Click **Settings**.

6 From the **Transfer Settings** dialog box, click the **SQL** tab.

7 Open the dialog box by clicking the arrow ⟨ > ⟩ next to the field (for example, to open the Select dialog box, click the arrow button for the **Select** box)

Use this tab to create SQL queries for extracting data from IBM System i (AS/400) files. Type text directly into the text boxes, or click any of the buttons on the right to open a dialog box to build a query.

NOTE: From the **Transfer** dialog box, select at least one host file before you build your query. Reflection displays field information from the specified file to help you build the query.

If you need help building your SQL query, consult your SQL documentation.

Select	Start building your `SELECT` statement by specifying fields (or columns) to transfer.
Where	In this box, add a `WHERE` clause to your `SELECT` statement. Specify one or more conditions that must be met for a record to be transferred.
Order by	In this box, add an `ORDER BY` clause to your `SELECT` statement to sort the records resulting from the query. You can sort only by fields specified in your `SELECT` statement.
Group by	In this box, add a `GROUP BY` clause to your `SELECT` statement to specify how to group the resulting data after the requested calculation (function) is performed.
	This clause is necessary when a function and multiple fields are specified in your `SELECT` statement.

Having	In this box, add a `HAVING` clause to apply a condition to a function of the `SELECT` statement.
	To enable the **Having** box and dialog box, you must first add a `GROUP BY` clause.
Join by	In this box, add a `JOIN` clause to your `SELECT` statement to specify how you want data from multiple files or members combined.
	To enable the **Join by** box and dialog box, you must have selected multiple files or members on the Host side of the **Transfer** dialog box.
Return records with missing fields	When joining records from more than one file, there may be cases where a record cannot be found to complete the join.

Related Topics

- "Create an SQL Query" on page 682
- "IBM System i (AS/400) Transfer" on page 681

Select Dialog Box

Getting there

1 Open the Transfer Dialog box.

 The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
The Reflection Ribbon	On the **Session** tab, from the **Transfer** group, click **File Transfer**.
The Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**.
TouchUx	Tap the Wrench icon and then under **Tools**, select **File Transfer**.

2 If you are running a 3270 session, change the protocol to AS/400.

  2a Click **Settings**.

  2b From the **Protocol** list, select **AS/400**.

  2c Click **OK**.

3 Click **Show Host Files**. (It may be necessary to enter your user name and password.)

4 Select one or more host files from which to transfer data.

5 Click **Settings**.

6 From the **Transfer Settings** dialog box, click the **SQL** tab.

7 Open the dialog box by clicking the arrow ⟨ > ⟩ next to the field (for example, to open the Select dialog box, click the arrow button for the **Select** box)

Type directly into the statement box, or use the lists and buttons to build your SQL query.

Finished statement	Start building your `SELECT` statement by specifying fields (or columns) to transfer.
	If you don't enter anything, all fields will be transferred.
Functions	Use these SQL functions to perform calculations on fields.
Fields	This box displays the fields in the selected file(s). For more information about a field, hover your mouse over the field name.

Related Topics

- "Create an SQL Query" on page 682
- "SQL Tab (Transfer Settings Dialog Box)" on page 704

Where Dialog Box

Getting there

1 Open the Transfer Dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
The Reflection Ribbon	On the **Session** tab, from the **Transfer** group, click **File Transfer**.
The Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**.
TouchUx	Tap the Wrench icon and then under **Tools**, select **File Transfer**.

2 If you are running a 3270 session, change the protocol to AS/400.

   2a Click **Settings**.

   2b From the **Protocol** list, select **AS/400**.

   2c Click **OK**.

3 Click **Show Host Files**. (It may be necessary to enter your user name and password.)

4 Select one or more host files from which to transfer data.

5 Click **Settings**.

6 From the **Transfer Settings** dialog box, click the **SQL** tab.

7 Open the dialog box by clicking the arrow $\boxed{>}$ next to the field (for example, to open the Select dialog box, click the arrow button for the **Select** box)

Type directly into the statement box, or use the lists and buttons to build your SQL query.

Finished statement	In this box, add a `WHERE` clause to your `SELECT` statement. Specify one or more conditions that must be met for a record to be transferred.
Fields	This box displays the fields in the selected file(s). For more information about a field, hover your mouse over the field name.
Value	Type a value to test against as part of your condition.

Related Topics

- "Create an SQL Query" on page 682
- "SQL Tab (Transfer Settings Dialog Box)" on page 704

Order By Dialog Box

Getting there

1 Open the Transfer Dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
The Reflection Ribbon	On the **Session** tab, from the **Transfer** group, click **File Transfer**.
The Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**.
TouchUx	Tap the Wrench icon and then under **Tools**, select **File Transfer**.

2 If you are running a 3270 session, change the protocol to AS/400.

   2a Click **Settings**.

   2b From the **Protocol** list, select **AS/400**.

   2c Click **OK**.

3 Click **Show Host Files**. (It may be necessary to enter your user name and password.)

4 Select one or more host files from which to transfer data.

5 Click **Settings**.

6 From the **Transfer Settings** dialog box, click the **SQL** tab.

7 Open the dialog box by clicking the arrow $\boxed{>}$ next to the field (for example, to open the Select dialog box, click the arrow button for the **Select** box)

Type directly into the statement box, or use the lists and buttons to build your SQL query.

Finished statement	In this box, add an `ORDER BY` clause to your `SELECT` statement to sort the records resulting from the query. You can sort only by fields specified in your `SELECT` statement.
Functions	Use these SQL functions to perform calculations on fields.
Fields	This box displays the fields in the selected file(s). For more information about a field, hover your mouse over the field name.

Related Topics

- "Create an SQL Query" on page 682
- "SQL Tab (Transfer Settings Dialog Box)" on page 704

Group By Dialog Box

Getting there

1 Open the Transfer Dialog box.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
The Reflection Ribbon	On the **Session** tab, from the **Transfer** group, click **File Transfer**.
The Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**.
TouchUx	Tap the Wrench icon and then under **Tools**, select **File Transfer**.

2 If you are running a 3270 session, change the protocol to AS/400.

   2a Click **Settings**.

   2b From the **Protocol** list, select **AS/400**.

   2c Click **OK**.

3 Click **Show Host Files**. (It may be necessary to enter your user name and password.)

4 Select one or more host files from which to transfer data.

5 Click **Settings**.

6 From the **Transfer Settings** dialog box, click the **SQL** tab.

7 Open the dialog box by clicking the arrow ⟨ > ⟩ next to the field (for example, to open the Select dialog box, click the arrow button for the **Select** box)

Type directly into the statement box, or use the lists and buttons to build your SQL query.

Finished statement	In this box, add a `GROUP BY` clause to your `SELECT` statement to specify how to group the resulting data after the requested calculation (function) is performed. This clause is necessary when a function and multiple fields are specified in your `SELECT` statement.
Fields	This box displays the fields in the selected file(s). For more information about a field, hover your mouse over the field name.

Related Topics

Having Dialog Box

Getting there

1 Open the Transfer Dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
The Reflection Ribbon	On the **Session** tab, from the **Transfer** group, click **File Transfer**.
The Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**.
TouchUx	Tap the Wrench icon and then under **Tools**, select **File Transfer**.

2 If you are running a 3270 session, change the protocol to AS/400.

2a Click **Settings**.

2b From the **Protocol** list, select **AS/400**.

2c Click **OK**.

3 Click **Show Host Files**. (It may be necessary to enter your user name and password.)

4 Select one or more host files from which to transfer data.

5 Click **Settings**.

6 From the **Transfer Settings** dialog box, click the **SQL** tab.

7 Open the dialog box by clicking the arrow [>] next to the field (for example, to open the Select dialog box, click the arrow button for the **Select** box)

Type directly into the statement box, or use the lists and buttons to build your SQL query.

Finished statement	In this box, add a `HAVING` clause to apply a condition to a function of the `SELECT` statement.
Functions	Use these SQL functions to perform calculations on fields.
Fields	This box displays the fields in the selected file(s). For more information about a field, hover your mouse over the field name.
Value	Type a value to test against as part of your condition.

Related Topics

Join By Dialog Box

Getting there

1 Open the Transfer Dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
The Reflection Ribbon	On the **Session** tab, from the **Transfer** group, click **File Transfer**.
The Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**.
TouchUx	Tap the Wrench icon and then under **Tools**, select **File Transfer**.

2 If you are running a 3270 session, change the protocol to AS/400.

   2a Click **Settings**.

   2b From the **Protocol** list, select **AS/400**.

   2c Click **OK**.

3 Click **Show Host Files**. (It may be necessary to enter your user name and password.)

4 Select one or more host files from which to transfer data.

5 Click **Settings**.

6 From the **Transfer Settings** dialog box, click the **SQL** tab.

7 Open the dialog box by clicking the arrow [>] next to the field (for example, to open the Select dialog box, click the arrow button for the **Select** box)

Type directly into the **Joins** box, or use the lists and buttons to build your SQL query.

Joins	In this box, add a `JOIN` clause to your `SELECT` statement to specify how you want data from multiple files or members combined.
Fields	This box displays the fields in the selected file(s). For more information about a field, hover your mouse over the field name.
Tables	This box displays the files or members selected on the Host side of the **Transfer** dialog box.

Related Topics

FTP Tab (Transfer Settings Dialog Box)

Getting there

1 Open a 3270 or 5250 terminal session.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Session** ribbon, from the **Transfer** group, click the **Transfer Settings** launcher:
Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**. In the Transfer dialog box, click the **Settings** button.
TouchUx	Tap the Wrench icon and then under **Tools**, select **File Transfer**. In the Transfer dialog box, click the **Settings** button.

2 From the **Protocol** list, select **FTP**.

3 Click the **FTP** tab.

The options are:

Host name or IP address	Type the name or IP address of the FTP server to log on to.
Anonymous	Log on to the FTP server as a guest, with the user name `anonymous`.
Save password	Select to save your password in encrypted form in your session document file. (Passwords for anonymous connections are not encrypted). If you prefer not to store information about your password in your session file, clear this check box. If the password was previously saved, it is removed.

User name	Enter your user name as it is registered on the FTP server.
Password	Enter the password the FTP server associates with the user name registered on the FTP server.
	When the **Anonymous** check box is selected, a password appears in plain text, instead of asterisks (*), as you type it.
	If no password is expected, click **OK** to continue.
Use Windows credentials	Use your Windows credentials instead of your FTP server credentials to bypass being prompted when performing a data transfer.
	NOTE: This option can be used only with IBM AS/400 and IBM AS/400 (Format 0) server types.
Advanced	Click to open the **FTP Properties** dialog box, from which you can configure additional FTP transfer features.
Defaults	Sets all FTP settings to the defaults, including the settings you configure using the **Advanced** button.

Related Topics

Transferring Files with FTP

You can perform FTP file transfer from a terminal session using Reflection integrated FTP support, or you can launch the FTP Client.

With Reflection FTP, you can connect to an FTP server running on any supported host. Once connected, FTP is used to transfer files between your PC and the FTP server.

Related Topics

Use Integrated FTP Transfer

Integrated FTP transfer is available when you want to use the FTP protocol from within a terminal session.

NOTE: If the transfer is one you'll be performing regularly, you can save your transfer settings in a transfer request file.

To transfer files using the FTP protocol from within a terminal session

1 Open the File Transfer dialog box.

The steps depend on your .

User Interface Mode	Steps
The Reflection Ribbon	On the **Session** tab, from the **Transfer** group, click **File Transfer**.
Classic or Classic MDI	On the Tools menu, choose **Transfer File**.
The Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**.

2 Click the **Settings** button, and configure the file transfer settings.

For most situations, you can configure for file transfers by selecting a preset configuration in the **Protocol** tab.

3 From the **Protocol** list, select **FTP**.

4 Click the **FTP** tab, and configure the host and user name information.

This doesn't have to be the host you're logged on to.

5 (Optional) Click **Advanced** to configure additional FTP settings.

6 Click **OK**.

7 From the **Transfer** dialog box, under **Local,** do one of the following:

- Browse under **Local folders**, and then select one or more files from the list.

  -or-

- Type the path and filename into the **File names** box.

8 Under **Host** specify a host file using one of the following techniques:

- Click **Show host files**, and browse to select one or more host files.

  -or-

- Type the file information into the **File names** box.

NOTE: If Reflection is configured to use a character set that is not supported by your host, you cannot display host files using the **Show host files** button.

---

9 To initiate a file transfer, do one of the following:

- Click a **Transfer** button to move the file in the indicated direction.

  -or-

- Drag the source file, and then drop it on the desired destination file.

Related Topics

-
-

Launch the FTP Client from a Terminal Session

You can launch the FTP Client from the Windows Start menu or from a Reflection terminal session.

To launch the FTP Client from a terminal session

- Open FTP Client as follows:

  The steps depend on your .

User Interface Mode	Steps
Ribbon	On the **Session** tab, from the **Transfer**group, click **FTP Client**.
Reflection Browser	On the Reflection menu, choose **Tools**and then **FTP Client**.
TouchUx	On the **Reflection** menu, tap the Wrench icon, and then select **FTP Client**.

Related Topics

-
-
-

Transfer Dialog Box

Getting there

Start Reflection and log on to the host computer as usual.

The steps depend on your .

User Interface Mode	Steps
The Reflection Ribbon	On the **Session** tab, from the **Transfer** group, click **File Transfer**.
The Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**.
TouchUx	Tap the Wrench icon and then under **Tools**, select **File Transfer**.

The options are:

Local

File names	Type the path and filename of the file you want to transfer. Separate multiple filenames with commas. Standard PC wildcard characters are supported.
Local Folders	Browse for the folder containing the file or files you want to transfer.

Transfer

Transfer	Click a transfer button to move the file(s) in the indicated direction.
Transfer method	Select how data conversion should be handled. The options available depend on the file transfer protocol. For additional information, see "IBM System i (AS/400) Transfer Method Options" on page 683 and "Mainframe Transfer Method Options" on page 673.
If file exists	Select what to do when the transferred file already exists in the target location.
Record format	Select the record format to use for transfers to the host:

Select	To
Fixed	Force the host to create fixed-length records.
Undefined	Force the host to create files without a specific record format (this value is only relevant for TSO systems).
Variable	Force the host to create variable-length records and preserve the format of a binary file.
Default	Let the host determine the record format.

Settings	Click the Settings button, and configure the file transfer settings.
Transfer Request	Choose one of the following:

Select	To
Open	Load transfer settings that you have saved to a transfer request file.
Save	Save your current transfer configuration to a transfer request file

Host

File names	Type or select one or more host files for the transfer. Separate multiple filenames with commas.

Show Host Files	Click to display host files in a tree view. The display you see depends on the protocol you have selected. Reflection displays only those files that can be transferred using the currently selected transfer protocol.
	In 5250 sessions, when you click Show Host Files you are prompted for user name and password, unless you have configured these values from the **AS/400** tab of the **Transfer Settings** dialog box.
	Show Host Files is not available if you are transferring to and from a CICS host.
Refresh	Click to refresh the file list. This button appears in place of the **Show host files** button after you have displayed the host files.
Add Library	Click to view an additional library (you will need to provide the library name). This button appears only if you are connected to an AS/400 host, and you have displayed the host files.
Level	Click to open the New Level dialog box, where you can specify the high-level qualifier or qualifiers (or filter) of the host files to display.
	NOTE: This button appears only if you have configured File Transfer for a TSO host and you have displayed the host files.
	If you enter a filter that is a subset of the files in the current view, only the files matching the filter are displayed. If the filter is not a subset of the files in the current view, the files matching the filter are added to the view.

Related Topics

Saving and Repeating Transfers

If you perform the same transfers frequently, you can use transfer request files to save your transfer information. You can save information about single transfers or batch transfers.

Related Topics

Transfer Request Files

Using transfer request files, you can perform the same transfer (or transfers) again later, without having to specify files and options each time. You can save transfer request files using either the **Single** or **Batch** tab of the **Transfer** dialog box.

NOTE: When you save a transfer request file from the **Batch** tab, Reflection stores the direction of transfer for each saved transfer. Therefore, you might want to use the **Batch** tab to save your transfer configuration, even if you have transferred only one file. When you save transfer request files from the **Single** tab, the direction of transfer is not included in the transfer request file.

Related Topics

Create a Transfer Request File

Using transfer request files, you can perform the same transfer (or transfers) again later, without having to specify files and options each time.

To create a transfer request file

1 Open the File Transfer dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
The Reflection Ribbon	On the **Session** tab, from the **Transfer** group, click **File Transfer**.
Classic or Classic MDI	On the Tools menu, choose **Transfer File**.
The Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**.

2 From the **Transfer** dialog box, configure and perform the transfer you want to save.

NOTE: If your terminal session is an IBM 3270 session, you can transfer files only to or from the host that your session is connected to. If your terminal session is an IBM 5250 session, you can transfer files to or from other hosts.

---

3 Under **Transfer request**, click **Save**.

4 In the **File name** box, type a filename.

5 In the **Transfer** list, specify whether data is being sent to the PC from the host, or from the host to the PC.

This setting is not saved with the transfer request file.

6 Click **Save**.

In 5250 sessions, transfer request files use the extension .XTO; in 3270 sessions, transfer request files use the extension .MTO.

NOTE: When you save a transfer request file from the **Batch** tab, Reflection stores the direction of transfer for each saved transfer. Therefore, you might want to use the **Batch** tab to save your transfer configuration, even if you have transferred only one file. When you save transfer request files from the **Single** tab, the direction of transfer is not included in the transfer request file.

Related Topics

◆ "Open a Transfer Request File" on page 718

◆ "Batch Transfers" on page 719

Open a Transfer Request File

When you open a transfer request file, you load the options previously saved to that file. To use saved transfer request files, first open the **Transfer** dialog box. You can load transfer requests from either the **Single** tab or the **Batch** tab.

NOTE: In 5250 sessions, transfer request files use the extension .XTO; in 3270 sessions, transfer request files use the extension .MTO.

To open a transfer request file

1 Open the Transfer dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
The Reflection Ribbon	On the **Session** tab, from the **Transfer** group, click **File Transfer**.
Classic or Classic MDI	On the Tools menu, choose **Transfer File**.
The Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**.

2 From the **Transfer** dialog box (either tab), under **Transfer request**, click **Open**.

3 Select the transfer request file you want to open.

4 Click **Open**.

5 To initiate a file transfer, do one of the following:

◆ Click a **Transfer** button to move the file in the indicated direction.

-or-

◆ Drag the source file, and then drop it on the desired destination file.

Related Topics

◆ "Create a Transfer Request File" on page 717

Batch Transfers

If you routinely perform a group of transfer operations, you can create and save a list of transfers from the **Batch** tab of the **Transfer** dialog box. Your transfer information is saved to a transfer request file. You can then use the transfer request file to perform multiple transfers in a single operation.

Related Topics

- "Save a Batch Transfer" on page 719
- "Run a Batch Transfer" on page 720
- "Batch Tab (Transfer Dialog Box)" on page 721
- "Batch Wizard" on page 722
- "Transfer Request Files" on page 717

Save a Batch Transfer

Using batch transfers, you can save a series of transfer operations to a single transfer request file. You can use this file later to repeat the same set of transfers.

NOTE: When you add an item to a batch, all aspects of the file transfer configuration are saved independently for each item, including file names, transfer direction, SQL query information, and any other transfer settings you have configured.

To create a batch transfer request file

1 Open the File Transfer dialog box.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
The Reflection Ribbon	On the **Session** tab, from the **Transfer** group, click **File Transfer**.
Classic or Classic MDI	On the Tools menu, choose **Transfer File**.
The Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**.

2 Click the **Settings** button, and configure the file transfer settings.

   NOTE: If your terminal session is an IBM 3270 session, you can transfer files only to or from the host that your session is connected to. If your terminal session is an IBM 5250 session, you can transfer files to or from other hosts.

   ---

3 Perform the series of transfers that you want to save to the batch.

   Successful transfers are automatically added to the batch list on the **Batch** tab.

   NOTE: If you prefer to configure transfers to be saved without actually transferring data, you can use the **Batch wizard** to add transfers to the batch list.

   ---

4 Click the **Batch** tab.

You can use this tab to modify individual items on the list, to add or delete items, and to change the order in which transfers occur when you run the saved file.

5 Click **Save**.

6 In the **File name** box, type a filename.

7 Click **Save**.

Related Topics

Run a Batch Transfer

1 Open the File Transfer dialog box.

User Interface Mode	Steps
The Reflection Ribbon	On the **Session** tab, from the **Transfer** group, click **File Transfer**.
Classic or Classic MDI	On the Tools menu, choose **Transfer File**.
The Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**.

2 Click the **Batch** tab.

3 Click **Open**, select a transfer request file and click **Open**.

In 5250 sessions, transfer request files use the extension .XTO; in 3270 sessions, transfer request files use the extension .MTO.

NOTE: By default, all items are transferred each time you run a batch request. If there are individual items you don't want to transfer this time, clear the check box to the left of the filename.

4 Click **Run**.

Batch Tab (Transfer Dialog Box)

Getting there

Start Reflection and log on to the host computer as usual.

User Interface Mode	Steps
The Reflection Ribbon	On the **Session** tab, from the **Transfer** group, click **File Transfer**.
The Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**.
TouchUx	Tap the Wrench icon and then under **Tools**, select **File Transfer**.

Click the **Batch** tab.

From the **Batch** tab, you can save file transfers for future use. Reflection saves batch transfers to transfer request files, and automatically adds successful transfers to the **Transfer list** on the **Batch** tab. You can also add file transfers using the Batch wizard.

Run	Perform all of the selected transfers in the list, starting at the top.
Add	Use the **Batch wizard** to add items to the list.
Remove	Delete the selected transfer.
Properties	Use the **Batch wizard** to view or modify the selected transfer. Changes you make using the **Batch wizard** affect the currently selected transfer only.
Move up	Move the selected item in the list.
Move down	Move the selected item in the list.
Open	Use the **Open Transfer Request File** dialog box to import transfers from an existing file. **NOTE:** Opening a transfer request file will replace any items currently in your list of transfers. Use the **Add** button to append additional items and keep the items in your current list.
Save	Save the items in your transfer list to a transfer request file.

Related Topics

- "Batch Transfers" on page 719
- "Send Files to a Mainframe" on page 670
- "Receive Files from a Mainframe" on page 672
- "Mainframe File Transfer" on page 670
- "Configure File Transfer" on page 684
- "Saving and Repeating Transfers" on page 717
- "Create a File Transfer Template" on page 675
- "Transfer Request Files" on page 717
- "Use File Transfer Naming Templates" on page 674
- "IBM System i (AS/400) Transfer" on page 681

Batch Wizard

Getting there

1 Open a 3270 or 5250 terminal session.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
The Reflection Ribbon	On the **Session** tab, from the **Transfer**group, click **File Transfer**.
The Reflection Browser	On the Reflection menu, choose **Tools**and then **File Transfer**.
TouchUx	Tap the Wrench icon and then under **Tools**, select **File Transfer**.

2 Click the **Batch** tab.

3 Click the **Add** button.

Use the **Batch wizard** to add new items to a batch transfer.

NOTE: Reflection automatically adds file transfers to your batch list when you transfer files from the **Single** tab of the **Transfer** dialog box. Adding items this way may suit your needs better than using the **Batch wizard.** The **Batch wizard** is useful when you want to add transfers to a batch without actually performing the transfer.

Add a new single transfer to batch	Use this option to configure a new transfer for the batch list. Click **Next** to configure the transfer using the **Batch Wizard** transfer panel (described below).
Host name	Specify the host to use for this transfer. If your terminal session is an IBM 3270 session, you can transfer files only to or from the host that your session is connected to. If your terminal session is an IBM 5250 session, you can transfer files to or from other hosts.
Transfer type	Select the file transfer protocol you want to use.
Add transfers from an existing batch file	Use this option to import transfers that you have already saved to a transfer request file. Transfers in the saved file are appended to the end of the current list.
Batch file name	Type path and filename of the transfer request file containing the transfer(s) you want to add to the batch.

Batch Wizard Transfer Panel

Use this panel to configure a transfer in your batch list. The **Batch Wizard** panel is similar to the **Single** tab of the **Transfer** dialog box, but has the following differences:

 ◆ Changes you make using the **Batch Wizard** panel affect only the item you are adding or modifying in the batch list; these changes have no affect on subsequent transfers and are not saved when you save your settings file.

 ◆ In the **Batch wizard**, you set the transfer direction by clicking **Send** or **Receive**. Your choice is indicated by the direction of the blue arrow at the top of the panel. No transfer actually occurs.

 ◆ The **Batch Wizard** panel includes a **Test** button that performs the currently configured transfer.

Related Topics

VT File Transfer

You can transfer files in Reflection using the **File Transfer** command from the **Transfer** group on the **Session** ribbon. You can transfer any type of file to and from a host computer. Use Reflection to transfer files between your PC and an HP 3000 (including Classic, MPE/iX, and POSIX), VMS (including OpenVMS and Alpha computers), ULTRIX, Unisys, Linux Console or UNIX system. Or, transfer files to any host or electronic service that supports the FTP, Zmodem, Xmodem, Kermit, or SuperKermit protocols.

Reflection includes its own proprietary protocol, called the WRQ/Reflection protocol. Before you can transfer a file for the first time, your administrator must upload the host file transfer program. Host programs are provided for HP 3000, VAX/VMS (DEC), AXP machines, and UNIX operating systems. A system administrator may have already uploaded the host program; if so, you can skip this step.

In this Section

Transfer a File

The **Transfer** dialog box supports two "drag-and-drop" methods for transferring files, in addition to specifying files and using the directional **Transfer** buttons.

Before you can transfer a file for the first time, your administrator must upload the host file transfer program.

To transfer a file

1 Open the File Transfer dialog box.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
The Reflection Ribbon	On the **Session** tab, from the **Transfer** group, click **File Transfer**.
Classic or Classic MDI	On the Tools menu, choose **Transfer File**.
The Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**.

2 From the **Transfer** dialog box, select a **Protocol**.

3 Select a **Transfer type**.

4 Select the action you want to occur if the transferred file exists in the target location.

   For more information about the options available, see the "Transferring Existing Files" on page 727 topic.

5 Click the **Settings** button, and configure the file transfer settings.

   For most situations, you can configure for file transfers by selecting a preset configuration in the **Protocol** tab.

6 Click **OK**.

7 Perform the file transfer using one of the following methods:

   ◆ Drag one or more files directly from Windows Explorer to the Host icon in the **Transfer** dialog box (or from the **Host file names** list to Windows Explorer).

      -or-

   ◆ Drag one or more files between the **Local** and **Host** boxes in the **Transfer** dialog box.

      -or-

   ◆ Type one or more filename(s) in the text boxes, and then click one of the **Transfer** buttons.

      For more information about the filenaming options available, see the "Filenaming and Wildcards" on page 732 topic.

   When the transfer begins, the **File Transfer in Progress** window opens. When transferring multiple files, this window displays the name of each file as it is being transferred; when the **If file exists** option is set to **Cancel** or there is some other error that stops the transfer, any remaining files matching a wildcard specification are not transferred. To cancel a file transfer in progress, click the **Cancel** button, press ESC, or press SPACEBAR.

Related Topics

◆ "Transfer Protocols" on page 725
◆ "Transfer Types" on page 731
◆ "Transferring Existing Files" on page 727
◆ "Filenaming and Wildcards" on page 732
◆ "Transfer Dialog Box (VT and HP)" on page 735
◆ "Configure File Transfer" on page 740

Transfer Protocols

A file transfer protocol is a set of rules that two computers follow for transferring files between them. Files can be transferred only when both computers use the same protocol. Protocols can specify error-checking and correction rules to ensure that the information you're transferring is accurately sent and received. Reflection supports several file transfer protocols:

- Reflection 7-bit and 8-bit WRQ/Reflection protocol to HP 3000 hosts (PCLINK2), VMS hosts (VAXLINK2), and to UNIX hosts (UNXLINK2)
- The FTP public domain protocol
- Zmodem public domain protocol
- Kermit public domain protocol
- Xmodem public domain protocol

If you use SuperKermit, Kermit, Zmodem, or Xmodem, that protocol must be available on the host, and you must start the host side of the process to transfer files.

On bulletin boards, you must issue a download or upload command before starting the transfer in Reflection.

WRQ/Reflection

The WRQ/Reflection protocol requires that the appropriate host program be on the host. These host programs include PCLINK2 on an HP 3000, VAXLINK2 on a VMS host, (including OpenVMS and Alpha computers), or UNXLINK2 for a UNIX host. The WRQ/Reflection protocol offers the following features:

- Wildcard transfers can be performed in either direction.
- CRC-CCITT error checking is used to ensure error-free transmission. Using this method, blocks are retransmitted, if necessary, to ensure completely accurate transmission.
- When you transfer a host file, all the file parameters of the host can be kept on the PC copy. This information can later be used to create an exact copy of the original file on the host.
- You can specify data translation parameters and many file transfer settings in the **Transfer Settings** dialog box.
- Data compression techniques produce faster transfers.

When Reflection is using the fast file transfer capability, data compression is not used because it usually slows down the file transfer.

- ASCII files can be sent from the PC to a host printer.
- When you click the **Attributes** button on the **WRQ** tab in the **Transfer Settings** dialog box or on the **Filter** tab, you can specify date/time filters (which limit the selection of files transferred using wildcards) or the file attributes for sending PC files and receiving host files.

FTP

File Transfer Protocol (FTP) is a public domain file transfer protocol used for file transfers to and from an FTP server. Because you can connect to an FTP server without an account, FTP servers can be useful to exchange a variety of files, including software upgrades and utilities.

Use FTP when you need network-speed file transfer across a terminal connection to a UNIX, HP 3000, VMS, or Unisys host.

If you will be using FTP exclusively for transferring files, use the Reflection FTP Client shipped with Reflection products. This application provides quick FTP transfers with a full complement of features.

Zmodem

Zmodem is a public domain file transfer protocol thatuses a 32-bit CRC (cyclic redundancy check) to detect transmission errors. It also allows for the batch transfer of more than one file, time and date stamping, and automatic downloading. TheZmodem protocol is often used for downloading and uploading files from bulletin boards.

Kermit

Kermit is a public domain file transfer protocol available for many types of computers. You can transfer files between a PC and a host running Kermit protocol. If the Kermit program on your host has a server mode, you can also use this mode to transfer files.

SuperKermit

The SuperKermit protocol offers the following enhanced features over the standard Kermit protocol:

- You can set packet sizes greater than 94bytes; the new default value is512, which results in faster transfers. You can set a packet size of up to2,048 bytes.
- The SuperKermit file transfer protocol is a sliding-window, or full-duplex protocol, which means that it sends data continuously while receiving occasional acknowledgments from the host.

In Reflection, you can set the number of packets that one side can receive before sending an acknowledgment. This value is 0-based, which means that the default setting of 1 (one) configures Reflection for a two-packet sliding-window under Kermit.

Xmodem

Xmodem is a public domain program used for file transfers, and is available for a variety of computers. The Xmodem binary transfer protocol transfers data in 128-byte data blocks. Reflection can receive a file in either 128-byte or 1K blocks, depending on the configuration of the remote system.

Most versions of Xmodem can perform CRC (cyclic redundancy check) error checking, which is accomplished when, from the **Transfer Settings** dialog box **Xmodem** tab, **Xmodem-CRC** is selected as the extension. This causes a 2-byte CRC and sets the packet size to 128-byte packets (not including overhead). The other two extension options are:

Xmodem	1-byte checksum, 128-byte packets
Xmodem-1K	2-byte CRC, 1024-byte packets

With the default **Extensions** option selected (**Xmodem-CRC**), on receives, Reflection automatically switches between **Xmodem-CRC** and **Xmodem-1K**, to match what the other end is sending.

Related Topics

- "Transfer a File" on page 724
- "Configure File Transfer" on page 740
- "Reflection FTP Client" on page 771

Transferring Existing Files

By default, Reflection asks you what to do if the local or host file being transferred already exists at the file transfer destination. If you don't want to be prompted for each existing file, you can change the **If file exists** option in the **Transfer** dialog box. The options provided by this feature will change depending on which protocol you are using.

The **If file exists** options apply to both sending and receiving files when you are using the WRQ/Reflection or FTP protocol. For all other protocols, the options only apply when you are receiving files from the host and the label of the option changes to **If local file exists**. When you are transferring files to the host, what happens to duplicate files depends on the operating system or protocol rules of the host.

NOTE: When you are transferring mixed or uppercase file names, keep in mind that some hosts recognize case as a distinguishing feature. Same-name files, such as Myfile.doc and MYFILE.DOC, can exist side-by-side in a folder on the host simply because they are capitalized differently.

When configuring Reflection file transfer in the **Transfer Settings** dialog box, you can select from several options to change the default behavior. If you select an option that is not available for all protocols, and then transfer a file using a protocol that does not support the default option, Reflection reverts to the **Ask User** setting.

The options are:

Append	Add the source file contents to the end of the destination file.
Ask User	Open a dialog box when the file already exists. The dialog box options change depending on the type of host to which you are connected and the protocol you are using.
Cancel	A transfer to the host is canceled only if a file with the specified name (and version number for VMS hosts) already exists. For VMS hosts, however, if you specify an existing filename without a version number, a new file with the same name is created, but with a version number one greater than the highest version number of the existing file. This applies to transfers from a PC to a VMS host, not to transfers from a host to a PC.
	If you send a file or files with the same name as an existing file to an HP 3000 or UNIX system, the transfer is canceled. If the file is part of a wildcard set (files being transferred using wildcards or a string of file names), no other files are transferred after a duplicate is found.
	When transferring a file to the PC, the file transfer is canceled when a file with the specified name already exists. If the file is part of a wildcard set (files being transferred using wildcards or a string of filenames), no other files are transferred to the PC after a duplicate is found.
Delete	When transferring to the PC, the existing file on the PC is deleted and a new file is created.
	When sending to a UNIX host (this option only applies to sending files to a UNIX host with the WRQ/Reflection protocol), a host file matching the local filename is deleted and a new file is created.

Overwrite	**For transfers to this host type**	**This option**
	HP	Replaces the data in the destination file but does not replace the attributes (characteristics) of the file.
		This can be a problem when overwriting a smaller file with a larger one; new records are not allocated to accommodate additional data, which means that only part of the file data is transferred.
	VMS	Replaces the most recent instance of the destination file.
	UNIX	Preserves existing symbolic links to the host file.

Purge

This option is available when you're using the WRQ/Reflection protocol, and when you're connected to a VMS host or an HP 3000 host. (With an HP 3000 host, this option is equivalent to deleting a file).

If you send a PC file to a VMS host using the **Purge** option, existing versions of the file on the host are purged following the transfer. For example, if you send `Notes.txt` to the host, and `Notes.txt;2` and `Notes.txt;3` already exist, a successful transfer results in a single file on the host called `Notes.txt;4`.

When transferring to the PC, the existing file on the PC is deleted and a new file is created.

Rename

Automatically make a copy of the existing file (you are not prompted). If you're connected to an HP 3000, the newly created file is renamed by inserting or appending three zeros, and then incrementing the numerical characters until a unique filename is created.

If 999 is reached and a unique filename is still not found, an error is returned.

For example, with a file named `filename`:

For MPE	**For POSIX**

```
  filenam0              filename000
  filenam1              filename001
  ...                   ...
  filenam9              filename009
  filena10              filename010
  filena11              filename011
  ...                   ...
  filena99              filename099
  filen100              filename100
  ...                   ...
  filen999              filename999
<error>               <error>
```

NOTE: For POSIX, the incremented numerical characters added to a filename will be inserted before any file extension, like this: `filename000.txt`.

Resume	Resume a cancelled transfer when Reflection encounters a file with the same name as that which you are transferring.
	This option is available only when you are using the Zmodem protocol, and works only when a previous attempt to receive the same file was interrupted and the **Delete cancelled receives** check box had been cleared.
Skip	Skip over the transfer of an existing file when one with the same name already exists (you are not prompted). If more files are to be transferred, they are processed after the skipped file.
	This option is only available when you're using the WRQ/Reflection or Zmodem protocol.
Update	(Applies only to the WRQ/Reflection protocol.) Update the existing file with the new one of the same name automatically (you are not prompted).
	If the file already exists on the host, the date and time stamp of the PC file is compared against the host's date and time stamp. If the host's date and time stamp precedes the PC's, the host file is purged and the PC file is transferred.
Use Remote	Use the disposition value specified by the remote system. If the remote system doesn't specify a disposition, the option defaults to **Ask User**.
	This option is only available when you're using the Zmodem protocol.

Related Topics

- "Confirm File Replace Dialog Box" on page 738

Transfer a File with Kermit

You can transfer files between a PC and a host running Kermit protocol. If the Kermit program on your host has a server mode, you can also use this mode to transfer files.

To transfer a file with Kermit protocol

1 Log in to the host and invoke the host Kermit program by typing `KERMIT` (or type in the string used by your particular version of Kermit) at the host prompt.

2 Prepare to transfer the file by typing either `RECEIVE` or `SEND <filename>` at the host's Kermit prompt. (These commands are from the host's point of view, so be sure to use `RECEIVE` when sending files to the host, and `SEND` when receiving files from the host.)

3 Open the File Transfer dialog box.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
The Reflection Ribbon	On the **Session** tab, from the **Transfer** group, click **File Transfer**.
Classic or Classic MDI	On the Tools menu, choose **Transfer File**.
The Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**.

4 From the **Protocol** list, choose **Kermit**.

5 Click the **Settings** button, and configure the file transfer settings.

6 From the **Preset configurations** list, select the type of host to which you're transferring, and then click **OK**.

7 Perform the file transfer.

To use Kermit server mode

1 Verify that the Kermit program on your host has a server mode.

2 After invoking Kermit on your host computer, put it in server mode by typing `SERVER` and pressing Enter.

3 Open the File Transfer dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
The Reflection Ribbon	On the **Session** tab, from the **Transfer** group, click **File Transfer**.
Classic or Classic MDI	On the Tools menu, choose **Transfer File**.
The Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**.

4 From the **Protocol** list, choose **Kermit**.

5 Click the **Settings** button, and configure the file transfer settings.

6 From the **Preset configurations** list, select **To Kermit Server**, and then click **OK**.

7 Perform the file transfer.

Related Topics

◆ "Transfer a File" on page 724

◆ "Kermit Tab (Transfer Settings Dialog Box)" on page 764

◆ "Transfer Protocols" on page 725

Transfer Types

The file transfer type determines the way the file is saved and any data manipulation that should be performed during the transfer. You can select from the following file transfer types: **ASCII**, **Binary**, **Labels** (HP 3000 host only), **Auto-Detect**, or **Image** (VMS host only). For protocols other than **WRQ/Reflection**, you can only select from **Binary** (the default), **ASCII**, or **Auto-Detect**.

NOTE: If you are transferring a file that contains double-byte characters, select **ASCII** or **Binary**, not **Auto-Detect**.

ASCII	Use to transfer text files with no special formatting.
	Data is transferred according to parameters set on the **Translation** tab in the **Transfer Settings** dialog box.

Binary	Use for program files and other types of files that should not be translated, such as files that have already been formatted for a particular type of printer or files with application-specific formatting. Binary files contain non-printable characters; using this method, a file is not converted or translated during the transfer.
Auto-detect	Use to cause Reflection to determine the file type and select the transfer type for you automatically (or to use your explicit association; see below).
	This option is especially useful when transferring mixed file types. Reflection uses the **Auto-detect** tab from the **Transfer Settings** dialog box to detect your preferred associations between file type (by its extension) and transfer method. The **Transfer Settings** dialog box contains common file type associations, any of which you can delete or move to another transfer type list.
Image	Use to transfer a VMS or UNIX program file between two hosts via the PC. When receiving files, attribute information is appended to the file stored on the PC; this information is then used to create the file when it is transferred back to the host. Therefore, when sending files, the file must first have been received on the PC from the host using the **Image** transfer type.
	In the case of VMS, the **Image** transfer type preserves the file's Record Management Services (RMS) attributes, such as the file's organization and record type. VMS files that are re-created correctly when transferred as image files include:

- .obj files
- .exe files
- .mai files
- Indexed files

  For UNIX, this preserves the UNIX file's user, group, and mode information.

Related Topics

- "Transfer a File" on page 724
- "Transfer Protocols" on page 725
- "Transfer Dialog Box (VT and HP)" on page 735

Filenaming and Wildcards

The list below describes the rules and behavior of filenames and wildcards in the **Transfer** dialog box for VT sessions.

- In the **Local file names** box, you can include a drive specifier, path name, and extension. However, the combination with filename (the path) cannot exceed 260 characters total. Local filenames are optional if you are receiving files from the host. Using the WRQ/Reflection protocol, wildcards can specify a group of PC files to send to the host.

- In the **Host file names** box, names must satisfy host system rules. For transfers to a VMS host, you can enter logical names. Host filenames are optional if you are sending files to the host.

- Specifying a filename supersedes any settings under **File name translation options** on the **Translation** tab of the **Transfer Settings** dialog box. Using the WRQ/Reflection protocol, host wildcard characters can specify a group of host files to send to the PC.

- You can also put wildcard entries in the text box. The receiving-side text box must be empty (or you can specify a path); host filename switches are allowed for VMS hosts. Then, click a **Transfer** button. The files are given the same names as they have on the sending end. All files transferred using wildcards use the specified values in the **Transfer** dialog box. Sets of ASCII and binary files should be transferred separately, or using auto-detect.

- The wildcard characters you use must be recognized as such by the computer that is transferring the files. The following table lists a few of the most common wildcard characters:

This computer	Recognizes these wildcards
PC, UNIX, VMS	* ?
HP 3000	@ ?

- When the transfer begins, the **File Transfer in Progress** window opens. When transferring multiple files, this window displays the name of each file as it is being transferred; when the **If file exists** option is set to **Cancel** or there is some other error that stops the transfer, any remaining files matching a wildcard specification are not transferred. To cancel a file transfer in progress, click the **Cancel** button, press ESC, or press SPACEBAR.

OpenVMS Host Filename Switches

Using the WRQ/Reflection protocol, you can specify various qualifiers, or switches, to modify the way the file is saved on the VAX, and how it is handled when the transfer is complete.

To use the file transfer switches, append the switch you want to the name of the host file when transferring it; for example to submit the file `Harriet.dat` to the print spooler after sending it to the VAX, from the **Transfer** dialog box, in the **Host file name** box, you would enter the following:

`Harriet.dat/S`

CAUTION: Do not type a space before appending a switch to a filename. Doing so results in an error — Reflection considers this as two separate filenames. For example, *Filename* `/A` is valid, whereas *Filename* `/A` will cause the transfer to fail.

The following switches are available:

Switch	Description	Remarks
/A	ASCII transfer: Set maximum record length	When transferring ASCII files with **Fast file transfer**, you can specify that the maximum record length be set in the file header of the resulting host file.

Switch	Description	Remarks
/B	Block mode	For binary transfers from the host only. Forces VAXLINK2 to read the host file in block mode rather than record mode. For certain files in non-standard formats, this gives you every byte that is actually contained in the file, including record separators, without regard to record lengths or carriage control. In other words, if you do a binary receive of a file that does not have fixed record lengths, record separators will be discarded unless you use /B. You must use this switch when the file was put onto the OpenVMS system using the Pathworks COPY command.
/C	Submit files to batch queue	File transfer to the host only. Submits the file or files to the batch queue (SYS$BATCH) upon completion of the transfer. Files are deleted on the host after they have been submitted; use /K to retain the file(s).
/D	DECDx format files	Binary file transfer only. Transfers files in DECDx format between the VAX and PC.
/F	Fixed length records	Formerly used with VAXLINK to specify fixed length binary files. VAXLINK2 creates this file format by default (this switch is offered only for backward compatibility with the older protocol).
/I	Image transfer method	Formerly used with VAXLINK to specify a file transfer type of image; the image method should be specified in the **Transfer** dialog box (this switch is offered only for backward compatibility with the older protocol).
/K	Keep submitted files	Valid only in conjunction with the /C or /S switch, both of which submit files to a queue on the host. Once the files are in the queue, they are typically deleted. To retain a copy of the file on the host, use the /K (keep) switch.
/L	Add linefeed	Binary file transfers from the host only. Appends a linefeed character to each record when receiving a file that has carriage control. The linefeed character is added even if the carriage control is not stream-lf.
/P	Translate carriage control characters	ASCII or binary file transfers from the host only. This switch translates FORTRAN or PRINT carriage control characters in OpenVMS files. When carriage control characters are not translated, they become part of the file's records. To discard these characters, use the /T switch.
/S	Spool files to printer	ASCII file transfers to the host only. Submits the file or files to the print queue (SYS$PRINT) upon completion of the transfer. Files are deleted on the host after they have been submitted; use /K to retain the file after it is submitted.
/T	Discard carriage control characters	ASCII or binary file transfers from the host only. Discards FORTRAN or PRINT carriage control characters in OpenVMS files. To translate these characters, use /P.
/V	Variable host record size	Binary file transfers to the host only. Creates the host file with variable-length records (the default is fixed).

Switch	Description	Remarks
/W	Block mode binary	Binary file transfers from the host only. Supports the block mode binary transfer required for files created by applications, such as the DOS and OpenVMS versions of Lotus 1-2-3 and WordPerfect.

Transferring Files with FTP

You can perform FTP file transfer from a terminal session using Reflection integrated FTP support, or you can launch the FTP Client.

With Reflection FTP, you can connect to an FTP server running on any supported host. Once connected, FTP is used to transfer files between your PC and the FTP server.

Related Topics

- "Transfer a File" on page 724
- "Configure File Transfer" on page 740
- "FTP Tab (Transfer Settings Dialog Box)" on page 768
- "Reflection FTP Client" on page 771

Launch the FTP Client from a Terminal Session

You can launch the FTP Client from the Windows Start menu or from a Reflection terminal session.

To launch the FTP Client from a terminal session

- Open FTP Client as follows:

  The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Session** tab, from the **Transfer** group, click **FTP Client**.
Reflection Browser	On the Reflection menu, choose **Tools** and then **FTP Client**.
TouchUx	On the **Reflection** menu, tap the Wrench icon, and then select **FTP Client**.

Related Topics

- "Transferring Files with FTP" on page 735
- "Reflection FTP Client" on page 771

Transfer Dialog Box (VT and HP)

Getting there

Start Reflection and log on to the host computer as usual.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
The Reflection Ribbon	On the **Session** tab, from the **Transfer** group, click **File Transfer**.
The Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**.
TouchUx	Tap the Wrench icon and then under **Tools**, select **File Transfer**.

The options are:

Local

File names	Type the path and filename of the file you want to transfer. Separate multiple filenames with commas. Standard PC wildcard characters are supported.
Local Folders	Browse for the folder containing the file or files you want to transfer.
Transfer	Click a transfer button to move the file(s) in the indicated direction.
Protocol	Select the file transfer protocol you want to use.
	For more information, see the "Transfer Protocols" on page 725 topic.
Transfer type	Select the desired transfer type. The file transfer type determines the way the file is saved and any data manipulation that should be performed during the transfer.
	For more information, see the "Transfer Types" on page 731 topic.
If file exists	Select what to do when the transferred file already exists in the target location.
	For more information, see the "Transferring Existing Files" on page 727 topic.
Host record size	**NOTE:** This box is only visible when you select, from the **General** tab of the **Transfer Settings** dialog box, **Show record size on > File Transfer dialog box**.
	Type a value between 0 and 32767 (default: 0).
	This value serves as an upper limit for the amount of data to be placed in the records of a file; records that exceed the maximum record size are split into multiple records. A value of 0 indicates that the host should determine the record size based on the transfer method selected (there is no maximum for ASCII transfers; 512-byte records are used for binary transfers). If you are in doubt as to a file's size, review other host files used by the same program.
	If you're using Reflection for HP with NS/VT to perform transfers to an HP host, ASCII transfers default to 80 bytes, and binary transfers default to 244 bytes (122 words on the host).
Settings	Click to configure the file transfer settings.
	For more information, see the "Configure File Transfer" on page 740 topic.

View Log	Click to open the log file specified on the **Logging** tab of the **Transfer Settings** dialog box.

Host

File names	Type or select one or more host files for the transfer. Separate multiple filenames with commas.
	When transferring a file to a VMS host, the filename does not have to be unique. However, only the latest version of the file is displayed in the file list (the one with the highest version number).
	If you want to transfer an earlier version of the file, you must type the name and version number in the **Host file names** box.
Show Host Files	(Applies to WRQ/Reflection and FTP protocols only.) Click to display a list of the files in the current directory on the host.
	Reflection first checks for a host connection, and then performs a file transfer to download a current listing of the files on the host.
	After you have clicked **Show Host Files**, the button changes to **Refresh Host Files**.
	If you add a new directory to the host, it will not display in the listing until you log on again.
Refresh Host Files	Click to confirm receipt of any files you transferred from the PC to the host, and to update the host file list.
	By default, the host file list is not updated automatically after a file transfer. However, you can change this behavior by selecting, from the **Transfer Settings** dialog box **General** tab, **Auto refresh host directory**.
Host directories	(Applies to WRQ/Reflection and FTP protocols only). Click to display a list of the host directories.
	To change to a different host directory, double-click its name. The list of files under **File Names** is updated appropriately.

NOTE: You can choose the same view of your files as you would in Windows Explorer by right-clicking either the **Local file names** or **Host file names** list, and choosing one of the options from the **View** menu: **Large Icons**, **Small Icons**, **List**, or **Details**.

Related Topics

FTP Log In Dialog Box

This dialog box opens when you have logged on to an FTP server without specifying a user name or password.

Enter Host (or System) Name or IP Address	Type the name or IP address of the FTP server to log on to.
User name	Enter your user name as it is registered on the FTP server. If you are logging in for the first time, try to log in as **Guest**, or log in by selecting the **Anonymous** check box.
Password	Enter the password the FTP server associates with the user name. When a password is expected and the **Anonymous** check box is selected, the password appears in plain text, instead of asterisks (*), as you type it. If no password is expected, click **OK** to continue.
	For added security, the number of asterisks that show do *NOT* match the number of characters in your password.
	Often, FTP servers expect an e-mail address as a password when you log in as an **Anonymous** user.
Anonymous	Log on to the FTP server as a guest, with the user name `anonymous`.

Confirm File Replace Dialog Box

This dialog box opens when the file you're receiving already exists. You are prompted because the **If local file exists** option is set to its default value of **Ask User**.

NOTE: Different protocols will have different text on this dialog box, and different file resolution options.

What would you like to do?	Select an option, and then click **OK**.
- or -	The options are described in the topic "Transferring Existing Files" on page 727.
File resolution	
Apply to all	Select an option, and then click **Apply to all** (or select the **Apply to all** check box and click **OK**).
	The existing file resolution option is applied to all of the files being transferred.
Cancel	Click to stop the transfer.

Related Topics

- "Transferring Existing Files" on page 727

Select Transfer Type Dialog Box

This dialog box opens when you receive a file with **Auto-Detect** as the transfer type, and **Scan** or **Ask user** are selected under **Transfer type for undefined extensions** from the **Auto-Detect** tab.

Transfer type	To continue the file transfer, select a transfer type and click **OK**.
Add extension to list	Select to transfer every file with this extension using the transfer type you selected from the **Transfer type** box. The selection is automatically updated from the **Auto-detect** tab.
	If you select this option for a file with no extension, you are adding an association between files with no extensions and the selected transfer type or method. Files with no extensions are listed on the **Auto-detect** tab as <>.

Auto-Detect Ask User Dialog Box

This dialog box opens when you transfer a file using the WRQ/Reflection protocol, and the **Transfer type** selected is Auto-detect, and the option for **If file exists** is Ask User.

Transfer type	To continue the file transfer, select a transfer type and click **OK**.
	Reflection automatically suggests the best option.
Add extension to list	Select to transfer every file with this extension using the transfer type you selected from the **Transfer type** box. The selection is automatically updated from the **Auto-detect** tab.
	If you select this option for a file with no extension, you are adding an association between files with no extensions and the selected transfer type or method. Files with no extensions are listed on the **Auto-detect** tab as <>.

Related Topics

- "Auto-Detect Tab (Transfer Settings Dialog Box)" on page 745
- "Transfer Types" on page 731

Add Auto-detect Extension Dialog Box

Getting there

1 Open a VT terminal session and then open the Transfer Settings dialog box.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Session** ribbon, from the **Transfer** group, click the **Transfer Settings** launcher: ⊡
Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**. In the Transfer dialog box, click the **Settings** button.
TouchUx	Tap the Wrench icon and then under **Tools**, select **File Transfer**. In the Transfer dialog box, click the **Settings** button.

2 From the **Transfer Settings** dialog box, click the **Auto-detect** tab.

3 Under **Auto-detect options**, click the **Add** button.

Type an extension, and then choose a transfer type to associate with that extension.

Extension	Type the extension for the transfer method. The limit is five characters, or type "<>" to associate a file with no extension to a transfer type.
Transfer type	Select a transfer type to associate with the extension in the **Extension** box.
	If you are unsure which transfer type to associate with an extension, use **Scan**. Reflection uses the proper transfer type after "scanning" the file being transferred.

Related Topics

◆ "Auto-Detect Tab (Transfer Settings Dialog Box)" on page 745

Configure File Transfer

You can manually configure file transfer settings by moving amongst the tabs in the **Transfer Settings** dialog box. Any configuration you perform is saved with your session document.

However, using the automated preset configurations is recommended.

To configure file transfer

1 Open the File Transfer dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
The Reflection Ribbon	On the **Session** tab, from the **Transfer** group, click **File Transfer**.
Classic or Classic MDI	On the Tools menu, choose **Transfer File**.
The Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**.

2 Click the **Settings** button, and configure the file transfer settings.

For most situations, you can configure for file transfers by selecting a preset configuration in the **Protocol** tab.

To see the contents of the predefined configuration, click the **View** button.

Related Topics

- "Transfer Dialog Box (VT and HP)" on page 735

Protocol Tab (Transfer Settings Dialog Box)

Getting there

1 Open the Transfer Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Session** ribbon, from the **Transfer** group, click the **Transfer Settings** launcher:
Classic or Classic MDI	On the Tools menu, choose **Transfer** File. Then, in the Transfer dialog box, click the **Settings** button.
Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**. In the Transfer dialog box, click the **Settings** button.

The protocol you select determines which preset configurations are available. Also, the tabs available from the **Transfer Settings** dialog box change to enable you to configure transfers using the selected protocol.

Protocol	Select the file transfer protocol you want to use. For information about the protocols, see the "Transfer Protocols" on page 725 topic.
Preset configurations	Selecting an item from this list adjusts the appropriate values automatically in the **Transfer Settings** dialog box for that specific environment. To see which values will change, select a preset configuration name and click **View**.
	To use the values you already have defined in Reflection (in the **Transfer Settings** dialog box and elsewhere), click **Current Configuration**. After doing so, the **View** button becomes unavailable.
View	Click to open the **View File Transfer Presets** dialog box, from which you can see the predefined settings for the currently selected preset configuration.

Related Topics

- "Configure File Transfer" on page 740
- "Transfer Protocols" on page 725

General Tab (Transfer Settings Dialog Box)

Getting there

1 Open the Transfer Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Session** ribbon, from the **Transfer** group, click the **Transfer Settings** launcher:
Classic or Classic MDI	On the Tools menu, choose **Transfer** File. Then, in the Transfer dialog box, click the **Settings** button.
Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**. In the Transfer dialog box, click the **Settings** button.

The options are:

General options

If file exists	Select a default for the **If file exists** setting on the **Transfer** dialog box. For more information, see the "Transferring Existing Files" on page 727 topic.
Start timeout	Set the maximum amount of time that Reflection should wait for a response from the host when starting a file transfer. If there is no response within the timeout period, an error message is displayed.
Receive timeout	Set the maximum amount of time that Reflection should wait for a block of data or an acknowledgment from the host when transferring a file. If there is no response within the timeout period, it is assumed that the data is lost and Reflection requests that it be sent again. Consecutive timeouts can cause termination of the file transfer (see **Error retry limit**).
Error retry limit	Set the number of times Reflection should try to transfer a block of data before abandoning the transfer.

Transfer dialog options

Show record size on File Transfer dialog box	(Applies only to the WRQ/Reflection protocol.) Select to display the **Host record size** box (located on the **WRQ** tab of the **Transfer Settings** dialog box, where it is labelled **Record size**) on the **Transfer** dialog box. This is convenient if you change the host record size often, and don't want to go to the **Transfer Settings** dialog box every time you need to change it.
Auto refresh host directory	Update the host directory display in the **Transfer** dialog box after you've sent a file. If you perform a large number of transfers, keeping this check box selected is not recommended because of the time it may require (depending on the number of files in the host directory) to query the host and then update this listing.
Display 8.3 filenames as	Select how you want filenames conforming to the DOS 8.3 file naming convention to display under **Local** in the **Transfer** dialog box. This option applies at all times when you use the WRQ/Reflection protocol, and also to Zmodem, XModem, Kermit, and FTP when the **File name translation** check box is selected on those protocol tabs in the **Transfer Settings** dialog box.

Download folder

The default folder in which received files should be placed	By default, Reflection specifies a folder associated with the current user. However, you can choose a different location. Type the full path, or use the **Browse** button.

Related Topics

Translation Tab (Transfer Settings Dialog Box)

Getting there

1 Open the Transfer Settings dialog box.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Session** ribbon, from the **Transfer** group, click the **Transfer Settings** launcher:
Classic or Classic MDI	On the Tools menu, choose **Transfer** File. Then, in the Transfer dialog box, click the **Settings** button.
Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**. In the Transfer dialog box, click the **Settings** button.

The options are:

Translation options for ASCII transfers

Translation to host

Change tabs to spaces	When selected, tab characters are expanded to spaces in the host file. Reflection replaces each tab character with the number of spaces necessary to fill out to the next tab stop, as specified in the **Spaces per tab** box. **NOTE:** This option is not related to the **Tabs** tab in the **Terminal Setup** dialog box.
Read CTRL-Z as end of file	When selected, file transfer uses Ctrl-Z as the end-of-file marker, and strips it from the file being sent. Otherwise, the character count in the file directory is used to determine the file length.

Translation from host

Change spaces to tabs	Select to use tab characters to replace consecutive spaces in the host file, and save local disk space. Reflection replaces consecutive spaces that fill out to the next tab stop, as specified by the **Spaces per tab** box, with a tab character. Many PC applications interpret embedded tabs as standard, 8-column tab stops. Clear this check box if your PC program cannot interpret embedded tabs to indicate column tab stops.
Write CTRL-Z at end of file	Select to add a Ctrl-Z (^Z) character to the end of a file when it is received. On the PC, ASCII text files normally end with ^Z, and many PC applications require this marker. This setting also affects whether an end-of-file marker is added in Reflection macros that use the `Open`, `PrintFile`, and `FlushPrinter` methods.
Delete trailing spaces	Select to save local disk space. Some host text files use fixed-length records to delimit lines; they pad the end of each record with blanks. Most PC text processing programs use a carriage return and linefeed sequence to delimit lines and paragraphs, and thus do not need blanks preceding a delimiter.
Spaces per tab	Set the number of tab stops used if you convert tabs to spaces.

Filename translation options

Change spaces to underscores when sending	Select to convert spaces in filenames to underscores in files sent to the host. If your host does not support spaces in filenames, this prevents the host from modifying the filename or rejecting the transfer. **NOTE:** This option is ignored if, from the **Transfer** dialog box, in the **Host file names** box, you type a new filename: the file is transferred and stored as you type it.

Change underscores to spaces when receiving	Select to convert underscores in filenames to spaces in files received from the host.
	By selecting this option in conjunction with the **Change spaces to underscores when sending** option, you satisfy the conventions of both the PC and the host, yet maintain the appearance of an unchanged file name: The name change occurs, but is transparent to both the PC and the host.
	This option applies at all times when you use the WRQ/Reflection protocol, and also applies to Kermit and Zmodem transfers when the **File name translation** check box is selected on the corresponding protocol tabs in the **Transfer Settings** dialog box.
	NOTE: This option is ignored if, from the **Transfer** dialog box, in the **Local file names** box, you type a new filename: the file is transferred and stored as you type it.
Truncate received filenames to 8.3 format	Select to receive host files in the DOS 8.3 filename format.
	For example, a file with the name `Longfilename.Document` will be converted automatically to `Longfile.doc` when transferred to your PC.
	This option applies at all times when you use the WRQ/Reflection protocol, and also applies to Kermit and Zmodem transfers when the **File name translation** check box is selected on the corresponding protocol tabs in the **Transfer Settings** dialog box.
	NOTE: This option is ignored if, from the **Transfer** dialog box, in the **Local file names** box, you type a new filename: the file is transferred and stored as you type it.

Related Topics

◆ "Configure File Transfer" on page 740

Auto-Detect Tab (Transfer Settings Dialog Box)

Getting there

1 Open the Transfer Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Session** ribbon, from the **Transfer** group, click the **Transfer Settings** launcher:
Classic or Classic MDI	On the Tools menu, choose **Transfer** File. Then, in the Transfer dialog box, click the **Settings** button.
Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**. In the Transfer dialog box, click the **Settings** button.

Use the **Auto-detect** tab to associate a filename extension (five characters or less) with a transfer type. When you send a file, it is transferred using the transfer type you specify.

Reflection comes with default extension associations. For example, the extension `.txt` is associated with the ASCII file type — when a `.txt` file is transferred, it is transferred as an ASCII file.

You can associate additional filename extensions with a file transfer type by clicking **Add**.

Auto-detect options

Add	Click to show the **Add Auto-detect Extension** dialog box, from which you can add filename extensions to a selected transfer type.
Remove	Click to remove the selected extension.
Transfer type for undefined extensions	To associate all files to this transfer method by default, select **ASCII**, **Binary**, **Image**, **Scan** or **Ask user**. Only those files that are already associated with a file transfer type are exempted.

If you are unsure about which transfer method to associate to the files you transfer, you have two choices:

- Select **Scan** to have Reflection determine the file transfer type without your input.

  -or-

- Select **Ask User**, and then from the **Ask User** dialog box, select the transfer method you want.

  NOTE: If you are transferring a file that contains double-byte characters, select **ASCII** or **Binary**, not **Scan**.

Related Topics

- "Add Auto-detect Extension Dialog Box" on page 739
- "Auto-Detect Ask User Dialog Box" on page 739
- "Transfer Types" on page 731
- "Configure File Transfer" on page 740

Logging Tab (Transfer Settings Dialog Box)

Getting there

1 Open the Transfer Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Session** ribbon, from the **Transfer** group, click the **Transfer Settings** launcher: 🖾
Classic or Classic MDI	On the Tools menu, choose **Transfer** File. Then, in the Transfer dialog box, click the **Settings** button.
Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**. In the Transfer dialog box, click the **Settings** button.

From this tab, you can enable logging for file transfer actions and specify the folder where the logging file should be created and updated. The logging file is named " `Transfer.log`" and will automatically rename itself by appending a number to the filename; for example, when the file exceeds 64K in size, it is renamed `Transfe1.log`. The older transfer information is retained in this now-renamed file and the file `Transfer.log` continues the process of adding transfer information.

Enable file transfer logging	Select to log file transfer information in a text file. The file includes information such as the transferred filename, the date and time, the protocol used, and whether the transfer was successful.
Log file name	Type the path and filename where the log file should be saved and updated.

Related Topics

- "Configure File Transfer" on page 740
- "Transfer Dialog Box (VT and HP)" on page 735

Filter Tab (Transfer Settings Dialog Box)

Getting there

1 Open a VT terminal session and then open the Transfer Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Session** ribbon, from the **Transfer** group, click the **Transfer Settings** launcher: 🖾
Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**. In the Transfer dialog box, click the **Settings** button.
TouchUx	Tap the Wrench icon and then under **Tools**, select **File Transfer**. In the Transfer dialog box, click the **Settings** button.

2 From the **Transfer Settings** dialog box, select either the WRQ/Reflection protocol or the FTP protocol.

3 Click the **Filter** tab.

From this tab, you can restrict which files are transferred, based on the date and time of their last modification. For example, to transfer only those files created after 5:00 p.m. on October 2nd, 2008, you would select the **Transfer files created after** check box, then enter:

```
Date:  10/02/08
Time:  17:00:00
```

The notation for the time and date depends on how you have the time set under the Regional Options in Windows Control Panel.

Transfer files created before	Select to specify a date and time, so that only files created before this time period are transferred.
Transfer files created after	Select to specify a date and time, so that only files created after this time period are transferred.
Exclude files	Exclude files from a file transfer by typing the filename(s) in this box. You can use wildcard characters; for example, to exclude HTML and GIF files, type the following:
	`*.htm, *.html, *.gif`

Related Topics

WRQ Tab (Transfer Settings Dialog Box)

Getting there

1 Open a VT terminal session and then open the Transfer Settings dialog box.

The steps depend on your .

User Interface Mode	Steps
Ribbon	On the **Session** ribbon, from the **Transfer** group, click the **Transfer Settings** launcher: [icon]
Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**. In the Transfer dialog box, click the **Settings** button.
TouchUx	Tap the Wrench icon and then under **Tools**, select **File Transfer**. In the Transfer dialog box, click the **Settings** button.

2 From the **Transfer Settings** dialog box, select the WRQ/Reflection protocol.

3 Click the **WRQ** tab.

The WRQ/Reflection protocol is proprietary to Reflection. Before you can transfer a file for the first time, your administrator must upload the host file transfer program.

WRQ/Reflection Protocol Options

Transfer type

When you perform a file transfer, it defaults to the transfer type you select from this list.

Select	To do this
ASCII	Apply the items under **Translation options for ASCII transfers** (set from the **Translation** tab) to be applied to the file contents, as well as any character set translation that you have opted to perform.
Binary	Transfer the file contents unchanged.
Image	Transfer between two host computers and preserve OpenVMS-specific information.
Auto-Detect	Have Reflection select the transfer type for you.

Transfer link

NOTE: If you're using **Fast file transfer**, this value is ignored.

Unless you're having trouble transferring files, keep this option set to its default value of **8-Bit** (this results in the fastest file transfer). In some environments, however, you may need to use one of the slower methods that convert non-printable ASCII characters to printable (and more reliably transferred) ASCII characters. Any conversion that takes place is reversed at the other end, so the contents of the file are unaffected.

For more information, see the topic.

Frame size

NOTE: If you're using **Fast file transfer**, this value is ignored.

Set the number of bytes of data to transfer at a time. The transfer program breaks a file into packets, or frames, that are sent one at a time until the entire file has been transmitted. There is no correlation between this box and the size of the records or blocks on the host computer.

A large frame size is more efficient when there are few transmission errors. This is especially important if you're communicating to the host over a modem, which has a greater chance of error. Use the default value in most situations.

Too small a frame results in long transmission times because of the overhead that occurs for each frame. Conversely, too large a frame can increase the elapsed time; when an error occurs, retransmitting a large frame takes longer.

For UNIX file transfers, the Window size multiplied by the Frame size cannot exceed the system-imposed limit on the number of characters that can be stored in the input queue. This limit is dependent on the particular implementation, but is typically at least 256.

Window size	**NOTE:** If you're using **Fast file transfer**, this value is ignored.
	The WRQ/Reflection file transfer protocol is a sliding-window protocol, which means that you can set the number of packets that one side sends before receiving an acknowledgment.
	For UNIX file transfers, the Window size multiplied by the Frame size cannot exceed the system-imposed limit on the number of characters that can be stored in the input queue. This limit is dependent on the particular implementation, but is typically at least 256.
	Because of host limitations, sliding windows are not supported by the HP 3000. For HP 3000 hosts, a window size of 1is always used, regardless of the actual setting here.
Preserve file date	Select to specify that, whenever a file is transferred, it should receive the source file's date and time, rather than the current date and time.
	The date used is the source file's last modification date, not the creation date.
Fast file transfer	**NOTE:** This option is not available when you have UNIX selected as the **System type**. It is only available when your host connection is through a network using the TELNET, LAT, or NS/VT protocols.
	When set to **Negotiate**, Reflection uses fast file transfer whenever possible, but reverts back to the standard protocol if fast file transfer is unsuccessful.
	When **Fast file transfer** is set to **Always**(or **Negotiate**, and it has been determined that fast file transfers can be performed), the following settings are ignored:
	``
	WRQEndCharacter
	WRQExtraCharacters
	WRQFrameSize
	WRQTransferLink
	WRQStartCharacter
	WRQWindowSize
	``
	It may be necessary to set this list to **Never** when sending ASCII files with records larger than 32,764 bytes.
Compress fast file transfer	If you have a fast network but comparatively slow CPU, clear this option to prevent **Fast file transfer** from using compression. However, if you have one of the faster CPUs currently available in today's market (for both PCs and hosts), select this option to speed up fast file transfer.
Compression	**NOTE:** If you're using **Fast file transfer**, this value is ignored.
	File compression typically speeds up file transfers. **Huffman** compression uses more processing power on the host and the local computer, but compresses data most effectively. Users with less computing power might prefer to select **Run Length** or **None** to bypass compression completely.

Record Separator	Opens the **Configure Record Separator** dialog box, from which you can set the line terminator characters to use on the host and on the PC.
	NOTE: Record separator options apply only to ASCII transfers.
	A record separator is a character string that signifies the end of a data stream, or record. Which character string serves as a record separator can vary according to the computer.

Host System Options

Startup command	Each time you start a file transfer using the WRQ/Reflection protocol, Reflection transmits the startup command to the host computer. This tells the host to run the Reflection file transfer program, using the name given when it was uploaded to the host.
	If you select a preset configuration (from the **Protocol** tab), the default command for the selected host type is inserted here.
System type	Select the type of host you will be sending files to or receiving files from.
Record size	**NOTE:** This option is not available when you have UNIX selected as the **System type**.
	Type a value between 0 and 32767 (default: 0).
	This value serves as an upper limit for the amount of data to be placed in the records of a file; records that exceed the maximum record size are split into multiple records. A value of 0 indicates that the host should determine the record size based on the transfer method selected (there is no maximum for ASCII transfers; 512-byte records are used for binary transfers). If you are in doubt as to a file's size, review other host files used by the same program.
	If you're using Reflection for HP with NS/VT to perform transfers to an HP host, ASCII transfers default to 80 bytes, and binary transfers default to 244 bytes (122 words on the host).
Save file attributes	Saves file attributes to your session document.
Attributes	Click to set file attributes specific to the selected system type.
Advanced	Click to set advanced file transfer options specific to the selected system type.

Related Topics

Transfer Link Options

Transfer link options can be set on the **WRQ** tab when configuring file transfer settings. In some environments, the default setting of 8-bit will not work, so you may need to use one of the slower methods that convert non-printable ASCII characters to printable (and more reliably transferred) ASCII characters

7-bit

Some host environments require translation of a wider variety of non-printable ASCII characters than those that are converted by the **8-Bit** option. If you have trouble with file transfers using Reflection and an intermediary system exists between your PC and the host computer (such as a gateway or router), using the **7-Bit** option may solve the problem.

When **7-Bit** is selected, each data character, including binary data, is examined and, if necessary, modified to ensure that it is a non-control (printable) ASCII character. This data modification is reversed by the recipient (the host computer or PC), so that the data being transferred is not affected. Each packet starts with an opening parenthesis — "(" — and ends with a closing parenthesis — ")".

8-bit

This value provides the fastest file transfers, because it converts only a small number of non-printable ASCII characters during a transfer. The following characters are translated:

Description	Character	Hex Value
Start of text	^B	02
End of text	^C	03
Carriage return	^M	0D
XON	^Q	11
XOFF	^S	13
End of medium	^Y	19
Number sign	#	23
Ampersand	&	26

UNIX file transfer translates the following additional characters:

Description	Character	Hex Value
Substitute	^Z	1A
Null	^@	00
Linefeed	^J	0A
Decimal 17	^Q	11
Decimal 19	^S	13
Decimal 128		80
Decimal 255		FF

If you need additional character translation beyond the default set of characters that is translated, select a different value from the **Transfer link** list.

Setting the **Transfer link** value to **8-Bit** requires an 8-bit data path. However, if you change **Parity** (in **Document Settings**, under **Configure Connection Settings**, click the **More Settings** button) to a value other than **8/None**, you no longer have an 8-bit data path and a **Transfer link** of **8-Bit** is ignored. All characters except those for the start and end of frame are converted.

User Defined

Some intermediate devices or drivers filter out a wider variety of non-printable ASCII characters than the default set of characters that are converted by the **8-Bit** option; this also applies to certain host applications and network environments.

If you create a macro for transfer presentation or start and end of frame characters using the command `WRQExtraCharacters,` and the properties you use do not correspond to the values for **8-Bit** or **7-Bit**, the **Transfer link** value automatically changes to **User Defined.**

Related Topics

- "WRQ Tab (Transfer Settings Dialog Box)" on page 748
- "Configure File Transfer" on page 740

Configure Record Separator Dialog Box

Getting there

1 Open a VT terminal session and then open the Transfer Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Session** ribbon, from the **Transfer** group, click the **Transfer Settings** launcher:
Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**. In the Transfer dialog box, click the **Settings** button.
TouchUx	Tap the Wrench icon and then under **Tools**, select **File Transfer**. In the Transfer dialog box, click the **Settings** button.

2 From the **Transfer Settings** dialog box, select the WRQ/Reflection protocol.

3 Click the **WRQ** tab.

4 Under **WRQ/Reflection protocol options**, click **Record Separator**.

This dialog box applies only to ASCII file transfers using the WRQ/Reflection protocol.

A record separator is a character string that signifies the end of a data stream, or record. Which character string serves as a record separator can vary according to the computer.

To host

Translate record separator	Select to remove the record separators listed in the **PC record separator** box from the file, and replace them with the record separator appropriate for the host.
PC record separator	By default, the most common record separator for PCs, carriage return/line feed (`CR/LF`), is specified.
Insert special characters	Select to type the character string you want Reflection to interpret as your PC's record separator. The characters you type on your keyboard will appear in the **PC record separator** box.

From host

Translate record separator	Select to remove the record separators for the host from the file and replace them with the record separator in the **Host record separator**box.
Host record separator	By default, the most common record separator for PCs, carriage return/line feed (`CR/LF`), is specified.
Insert special characters	Select to type the character string you want Reflection to interpret as your PC's record separator. The characters you type on your keyboard will appear in the **Host record separator** box.

Related Topics

HP Advanced File Transfer Options Dialog Box

Getting there

1 Open a VT terminal session and then open the Transfer Settings dialog box.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Session** ribbon, from the **Transfer** group, click the **Transfer Settings** launcher:
Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**. In the Transfer dialog box, click the **Settings** button.
TouchUx	Tap the Wrench icon and then under **Tools**, select **File Transfer**. In the Transfer dialog box, click the **Settings** button.

2 From the **Transfer Settings** dialog box, select the WRQ/Reflection protocol.

3 Click the **WRQ** tab.

4 Under **Host system options**, from the **System type** list, choose an HP host.

5 Click the **Advanced** button.

The options are:

MPE file names	Select a naming format. For more information, see the "MPE File Names, WRQ protocol" on page 758 topic.
Send as stream	Native POSIX files under version 5.0 of the MPE operating system support a new record format known as "stream," which is just a stream of bytes. Files created under the POSIX shell or by POSIX programs have this format by default. Files created from the MPE command interpreter or by MPE programs can be stream files.
	Interoperability between stream files and other record formats is automatic. This means an MPE program can read from a stream file and it will appear to be a traditional variable length record file, and a POSIX program will see all files as stream files. MPE does the translation automatically.
	If you want all files that you send to the host to have the stream format, select **Send as stream** (when you receive files from the host, the WRQ/Reflection protocol automatically detects the record format of the host file and the correct translation is performed). When this option is cleared, PCLINK2 defaults to a **Fixed** record format for ASCII files and a **Variable** record format for binary files.
QEdit format on send	Select to create a host file with the QEdit format.
Send to spooled device	Select to send output to a spooled device on MPE/iX machines.
Remove file extension on send	Select to strip the filename extension automatically from the files you are sending to an HP 3000.

Related Topics

◆ "MPE File Names, WRQ protocol" on page 758

◆ "HP File Attributes Dialog Box" on page 756

HP File Attributes Dialog Box

Getting there

1 Open a VT terminal session and then open the Transfer Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Session** ribbon, from the **Transfer** group, click the **Transfer Settings** launcher:
Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**. In the Transfer dialog box, click the **Settings** button.
TouchUx	Tap the Wrench icon and then under **Tools**, select **File Transfer**. In the Transfer dialog box, click the **Settings** button.

2 From the **Transfer Settings** dialog box, select the WRQ/Reflection protocol.

3 Click the **WRQ** tab.

4 Under **Host system options**, from the **System type** list, choose an HP host.

5 Click the **Attributes** button.

NOTE: With the exception of **Carriage control** and **Domain**, HP file attributes affect only the transfer of new files to the host. When you send a file that already exists on the host, these specifications are ignored.

Specifying HP attributes is an alternative to explicitly creating a file equation for a new file on the host prior to the actual transfer. The HP file attributes are used to define the physical characteristics of the file when it is created on the host. If you specify invalid file attributes, the host will refuse the file transfer; and Reflection will display an error message.

File attributes

Blocking factor	Set the number of logical records to be contained in one physical block.
File code	Set the file code that identifies the file's purpose or format.
File extent	Set the maximum number of extents for the file.
Number of user labels	Set the number of user labels to be written for the file.
File size (in records)	Set the maximum file size.

Domain

Select the domain where the file resides. The domain specification determines which location, the system domain or the temporary file domain, the host uses during the transfer. For existing files, your specification should match the current domain specification for the file. If the specification does not match, a send results in a new file in the domain specified; the existing file remains unchanged in its domain.

Temporary	Select when transferring a temporary job file, which is retained in the temporary file domain for use during the current session.
Permanent	By default, the domain is set to **Permanent**; the file is located in the system domain.
Carriage control	When selected, carriage control characters are maintained in the first column of each line in the file. The first character of each line is assumed to be a carriage control, and it is retained as such.
	When cleared, it is assumed that no carriage control exists in the local file (and therefore nothing is discarded).

Record type

Select the type of file you're transferring.

ASCII	Create an ASCII file.
Binary	Create a binary file
Default	Use the value selected in the **Transfer type** list on the **WRQ** tab.

File type

Select the type of file to create on the host. **Standard** indicates that a regular file is always created on the host. The other types are created only if they are specified explicitly from this dialog box or in the file header of a labels transfer.

Record format

The setting **Default** creates a record format based on the **Send as Stream** setting from the **HP Advanced File Transfer Options** dialog box.

When	This occurs
Send as Stream is selected	A byte-stream file is created on the host (regardless of the transfer method).
Send as Stream is cleared	If the **Transfer** type is **ASCII**, a fixed-length ASCII file is created.
	-or-
	If the **Transfer** type is **Binary**, a variable-length binary file is created.

Related Topics

- "WRQ Tab (Transfer Settings Dialog Box)" on page 748
- "Configure File Transfer" on page 740

MPE File Names, WRQ protocol

This filename structure is used for host filenames during file transfers, and it also determines how the filenames display in the **Transfer** dialog box after clicking the **Show Host Files** button.

Reflection supports four name spaces for filenames:

- **Traditional MPE filenames.** The names are assumed to be all uppercase (regardless of how they are entered in the **Host file names** box), and each name is a maximum of eight characters in the format directory structure FILENAME.GROUP.ACCOUNT. When this list is set to **MPE**, files beginning with a period or a forward slash (. or /) are interpreted as POSIX files.
- **MPE/iX 5.x POSIX filenames.** For example, the names can be mixed case up to 32 characters in length, using a fully hierarchical directory structure.

MPE filenames are a subset of the POSIX names. All MPE filenames are visible from within **POSIX** (for example, PCLINK2.PUB.SYS appears as /SYS/PUB/PCLINK2), but only POSIX files whose names are also valid as MPE filenames are visible from **MPE**.

- When you select **Auto** from this list, the host will determine if it is running under the MPE Command Interpreter or the POSIX shell. If it is the MPE CI, the name space is set to **MPE**; if it is the shell, the name space is set to **POSIX**.

NOTE: Even though the host determines the name space, the setting in the dialog box is not changed; it remains as **Auto**.

- Selecting **MPE-Only** from this list allows only valid MPE names to be accepted. Filenames starting with "." or "/" are treated as errors.

This option is for those users who used the ".groupname" construct for the host filename. This allowed you to transfer files into a different account. For example, specifying ".PUB" transferred files into the "PUB" group. With the introduction of POSIX, this behavior changed. By default, PCLINK2 interprets the ".PUB" as a POSIX name and therefore attempts to transfer the files as a single file named ".PUB". If the name space is set to **MPE-Only**, the old behavior is performed.

There is an alternative to setting the name space to **MPE-Only**. If the name space is left set to **MPE**, then the host name may be specified as "@.groupname" as in "@.PUB". This will result in the same behavior as described above for the **MPE-Only** name space.

Related Topics

-
-
-

OpenVMS Advanced File Transfer Options Dialog Box

Getting there

1. Open a VT terminal session and then open the Transfer Settings dialog box.

   The steps depend on your .

User Interface Mode	Steps
Ribbon	On the **Session** ribbon, from the **Transfer** group, click the **Transfer Settings** launcher:
Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**. In the Transfer dialog box, click the **Settings** button.
TouchUx	Tap the Wrench icon and then under **Tools**, select **File Transfer**. In the Transfer dialog box, click the **Settings** button.

2 From the **Transfer Settings** dialog box, select the WRQ/Reflection protocol.

3 Click the **WRQ** tab.

4 Under **Host system options**, from the **System type** list, select **OpenVMS**.

5 Click the **Advanced** button.

Send options

Submit to print queue on send	Select to submit the file to the SYS$PRINT queue upon completion of the transfer. Once the file has been submitted to the print queue, it is automatically deleted on the host, unless the **Keep file after submitting** option is selected.
Submit to batch queue on send	Select to submit the file on the OpenVMS host to the SYS$BATCH queue upon completion of an ASCII transfer. Once the file has been submitted to the batch queue, it is automatically deleted on the host unless the **Keep file after submitting** option is selected.
Keep file after submitting	This option is unavailable (dimmed) unless either the **Submit to print queue** or **Submit to batch queue** is selected. Once the files are in the queue, they are deleted unless you select this option.
Preserve record counts	Select to transfer record byte counts with the data during a binary transfer to the host; this transfers files in DECDx format.

Receive options

Use block reads	Select to force VAXLINK2 to read the host file in block mode rather than record mode. For certain files in non-standard formats, this transfers every byte that is actually contained in the file, without regard to record lengths or carriage controls. It is equivalent to using the image transfer method but omitting the image header information.
Translate carriage control	Select to translate FORTRAN or PRINT carriage control characters in OpenVMS files. Without this setting, you can enable TranslateCharacters to prevent carriage control characters from being translated unpredictably. When carriage control characters are not translated, they become part of the file's records.

Related Topics

- "WRQ Tab (Transfer Settings Dialog Box)" on page 748
- "Configure File Transfer" on page 740

OpenVMS File Attributes Dialog Box

Getting there

1 Open a VT terminal session and then open the Transfer Settings dialog box.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Session** ribbon, from the **Transfer** group, click the **Transfer Settings** launcher:
Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**. In the Transfer dialog box, click the **Settings** button.
TouchUx	Tap the Wrench icon and then under **Tools**, select **File Transfer**. In the Transfer dialog box, click the **Settings** button.

2 From the **Transfer Settings** dialog box, select the WRQ/Reflection protocol.

3 Click the **WRQ** tab.

4 Under **Host system options**, from the **System type** list, select **OpenVMS**.

5 Click the **Attributes** button.

The options are:

File attributes

Record attributes	Select a record attribute from this list, or accept the default, which allows Reflection to examine the record and logically select the proper attribute for it.
No block span	By default, records are allowed to cross block boundaries. Select this option if you do not want records to cross block boundaries.
Record format	Select a record format from this list, or use the default, which allows the host program to determine the default record format based on the transfer method.
Control field size	Type the maximum record size. This box is available only when the **Record format** list is set to **Variable w/ fixed Ctrl**.
Allocation	Type the number of blocks initially allocated for the file at the time of creation. If you leave this box blank, or specify a value of 0, the entire file is preallocated.
File options	Select **Contiguous** to create a contiguous file (the transfer fails if it is not possible); select **Best-try contiguous** to create a contiguous file (if that is possible).

File protection

Assign the protection for a destination file. If no selections are made, protection for the file is determined by the host system.

To prevent access to all files, select the **No access** option.

Owner UIC	Type the Owner User Identification Code (UIC) for alternate owners of the file.

Related Topics

◆ "WRQ Tab (Transfer Settings Dialog Box)" on page 748

◆ "Configure File Transfer" on page 740

UNIX Advanced File Transfer Options Dialog Box

Getting there

1 Open a VT terminal session and then open the Transfer Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Session** ribbon, from the **Transfer** group, click the **Transfer Settings** launcher:
Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**. In the Transfer dialog box, click the **Settings** button.
TouchUx	Tap the Wrench icon and then under **Tools**, select **File Transfer**. In the Transfer dialog box, click the **Settings** button.

2 From the **Transfer Settings** dialog box, select the WRQ/Reflection protocol.

3 Click the **WRQ** tab.

4 Under **Host system options**, from the **System type** list, select **UNIX**.

5 Click the **Advanced** button.

The option is:

Show hidden files	Select to show hidden files on the UNIX host when the host directory list is displayed in the **Transfer** dialog box.

Related Topics

◆ "WRQ Tab (Transfer Settings Dialog Box)" on page 748

◆ "Configure File Transfer" on page 740

UNIX File Attributes Dialog Box

Getting there

1 Open a VT terminal session and then open the Transfer Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Session** ribbon, from the **Transfer** group, click the **Transfer Settings** launcher:
Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**. In the Transfer dialog box, click the **Settings** button.
TouchUx	Tap the Wrench icon and then under **Tools**, select **File Transfer**. In the Transfer dialog box, click the **Settings** button.

2 From the **Transfer Settings** dialog box, select the WRQ/Reflection protocol.

3 Click the **WRQ** tab.

4 Under **Host system options**, from the **System type** list, select **UNIX**.

5 Click the **Attributes** button.

The options are:

Owner	Type the file owner name in this box. The value must correspond to a valid login name or user ID in the specified group.
Group	Type the group of the file's owner in this box. The value must correspond to a valid group name or group ID.
Set mode	When selected, you're allowed to assign Read, Write, and Execute protection for Owner, Group, Others, and All. If the **Set mode** option is not selected, permissions are determined by the default creation mode on the host.
Set user ID on execution	When transferring an executable file, select to specify that the owner's permissions should determine access when the program is run (instead of using the permissions of the person running the program).
Set group ID on execution	Select to specify that the permissions of the login group of the person running the file determine access while the file is running. See chmod (1) in your UNIX documentation.
Save text image after execution	If an executable file is prepared for sharing, selecting this option prevents the system from abandoning the swap space image of the program-text portion of the file when its last user terminates. When the next user of a file executes it, the text does not need to be read from the file system (it is swapped in), thus saving time.

Related Topics

Zmodem Tab (Transfer Settings Dialog Box)

Getting there

1 Open a VT terminal session and then open the Transfer Settings dialog box.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Session** ribbon, from the **Transfer** group, click the **Transfer Settings** launcher:
Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**. In the Transfer dialog box, click the **Settings** button.
TouchUx	Tap the Wrench icon and then under **Tools**, select **File Transfer**. In the Transfer dialog box, click the **Settings** button.

2 From the **Transfer Settings** dialog box, select the Zmodem protocol.

3 Click the **Zmodem** tab.

The options are:

Transfer type	When you perform a file transfer, it defaults to the transfer type you select from this list.

Select	To do this
ASCII	Apply the items under **Translation options for ASCII transfers** (set from the **Translation** tab) to be applied to the file contents, as well as any character set translation that you have opted to perform.
Binary	Transfer the file contents unchanged.
Auto-Detect	Have Reflection select the transfer type for you.

Character set translation (ASCII)	When you perform an ASCII transfer with this option selected, Reflection translates characters based on the settings from the **Translation** tab of the **Transfer Settings** dialog box and the **Emulation** tab of the **Terminal Setup** dialog box.
File name translation	Select to invoke settings automatically under **File name translation options** on the **Translation** tab.
Packet size	Select or type the sub-packet size for file transfers. This value tells Zmodem how many bytes of data to transfer at a time.
	In many cases, the Zmodem protocol will adjust this value during a transfer as necessary (the value shown in this dialog box does not change).

Allow automatic downloading	If selected, when you initiate a send (from either a host system or bulletin board), Reflection immediately starts receiving a remote file with the same name as soon as it detects a Zmodem header. It is not necessary for the protocol to be set to **Zmodem** in the **Transfer** dialog box for this to happen. **NOTE:** With automatic downloading, you are not prompted for a filename or a transfer method.
Delete cancelled receives	Select to have a partially received file deleted automatically if you cancel the transfer in the middle of receiving a file. (If a download stop, but you did not cancel it, the received file is always kept.

Host system options

These startup commands are initiated from the host, which is why the term *receive* is used to describe the action of *sending* files to the host.

NOTE: These settings are necessary only when transferring files to and from a host system; they are not required for transferring files to and from a bulletin board.

Receive startup command	When you send a file, this command is transmitted to the host. Type the name of the program that starts Zmodem receives on the host. If you do not indicate a receive startup sequence, you must manually start the Zmodem receive program on the host before you can send the local file.
Send startup command	When you receive a file, this command, along with the name of the file to be received, is transmitted to the host. Type the name of the program that starts Zmodem sends on the host. If you do not indicate a send startup sequence, you must manually start the Zmodem send program on the host before you can receive the host file. For OpenVMS hosts, this sequence must be defined as a foreign command.

Related Topics

◆ "Configure File Transfer" on page 740

Kermit Tab (Transfer Settings Dialog Box)

Getting there

1 Open a VT terminal session and then open the Transfer Settings dialog box.

The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Session** ribbon, from the **Transfer** group, click the **Transfer Settings** launcher: 🖼
Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**. In the Transfer dialog box, click the **Settings** button.
TouchUx	Tap the Wrench icon and then under **Tools**, select **File Transfer**. In the Transfer dialog box, click the **Settings** button.

2 From the **Transfer Settings** dialog box, select the Kermit protocol.

3 Click the **Kermit** tab.

The options are:

Transfer type	When you perform a file transfer, it defaults to the transfer type you select from this list.

Select	To do this
ASCII	Apply the items under **Translation options for ASCII transfers** (set from the **Translation** tab) to be applied to the file contents, as well as any character set translation that you have opted to perform.
Binary	Transfer the file contents unchanged.
Auto-Detect	Have Reflection select the transfer type for you.

Checksum	Kermit supports three types of error checking: single-byte checksum, double-byte checksum, and 3-byte CRC. If the Kermit program at the other end of the transfer does not support the selected level, single-byte checksum is used. Single-byte is fastest, but CRC is safest.
Character set translation (ASCII)	When you perform an ASCII transfer with this option selected, Reflection translates characters based on the settings from the **Translation** tab of the **Transfer Settings** dialog box and the **Emulation** tab of the **Terminal Setup** dialog box.
File name translation	Select to invoke settings automatically under **File name translation options** on the **Translation** tab.

Automatic server mode	When selected, Reflection interacts with the host Kermit server program in the following manner:

- When you first open the **Transfer** dialog box, no interaction with the host occurs.

- When you request a Kermit transfer, the host is put into server mode by transmitting the Server Startup command. If you do not specify a sequence, Reflection updates its state to reflect that the host Kermit is in server mode. Reflection takes no other action.

- As long as the **Transfer** dialog box remains open, the host Kermit remains in server mode and transfers occur as you request them.

When **Automatic Server mode** is selected, any of the following actions shut down the host Kermit server program: closing the **Transfer** dialog box, clicking the **Setup**button, or changing the file transfer protocol.

SuperKermit Options

| Packet size | Select the requested packet size in bytes for Kermit transfers; this value tells the SuperKermit protocol how many bytes of data to transfer at a time. This value controls the packet size used for transfers *from* the host. For transfers *to* the host, the packet size set in the host's Kermit program is used. If the host Kermit server program does not support long packets, the packet size is set to 94 bytes. Programs that support packet sizes greater than 94 bytes are often designated SuperKermit programs.

In addition to the values available from the list box, you can also type in any value from 32 to 2,048. |
|---|---|
| Window size | If the remote Kermit program supports sliding windows, this parameter determines the size of a sliding window, in packets. This value is 0-based, so the default setting (1) configures Reflection for a two-packet sliding window. Programs that support sliding windows are often designated SuperKermit programs.

If the remote Kermit doesn't support sliding windows, Reflection reverts automatically to a window size of 0 (zero). |

Host system options

These startup commands are initiated from the host, which is why the term *receive* is used to describe the action of *sending* files to the host.

NOTE: These settings are only necessary when transferring files to and from a host system; they are not required for transferring files to and from a bulletin board.

Receive startup command	When you send a file, this command is transmitted to the host. Type the program name that starts Kermit receives on the host. If you do not indicate a receive startup sequence, you must manually start the Kermit receive program on host before you can send the local file.
	The $FILENAME macro can optionally be specified. If present, it is replaced with the filename or wildcard filespec of the file that the host is to send. Use the $FILENAME macro in cases where additional text needs to appear after the filename.
	You can embed the $BINARY:<string> macro in the command. This causes the specified <string> to be included in the transmitted startup sequence if the transfer type is binary; otherwise, the string is omitted. The <string> is defined as everything between $BINARY: and the next space.
Send startup command	When you receive a file, this command, along with the name of the file to be received, is transmitted to the host. Type the name of the program that starts Kermit sends on the host. If you do not indicate a send startup sequence, you must manually start the Kermit send program on the host before you can receive the host file.
	You can embed the $BINARY:<string> macro in the command. This causes the specified <string> to be included in the transmitted startup sequence if the transfer type is binary; otherwise, the string is omitted. The <string> is defined as everything between $BINARY: and the next space.
Server startup command	This command is used in conjunction with the **Automatic server mode** check box to allow Reflection to put the host Kermit in server mode automatically. This string, followed by a CR, is transmitted to the host when Reflection wants to put the host in server mode.

Related Topics

-
-

Xmodem Tab (Transfer Settings Dialog Box)

The options are:

Transfer type	When you perform a file transfer, it defaults to the transfer type you select from this list.

Select	To do this
ASCII	Apply the items under **Translation options for ASCII transfers** (set from the **Translation** tab) to be applied to the file contents, as well as any character set translation that you have opted to perform.

Binary	Transfer the file contents unchanged.
Auto-Detect	Have Reflection select the transfer type for you.
Character set translation (ASCII)	When you perform an ASCII transfer with this option selected, Reflection translates characters based on the settings from the **Translation** tab of the **Transfer Settings**dialog box and the **Emulation** tab of the **Terminal Setup** dialog box.
Extensions	There are two variables to be aware of with Xmodem: The error checking (1-byte checksum or 2-byte CRC) and the packet size (128 or 1024 bytes, not including overhead). With the default **Extensions**option selected, Reflection automatically switches between **Xmodem-CRC** and **Xmodem-1K** on receives to match what the other system is sending.

Related Topics

◆ "Configure File Transfer" on page 740

FTP Tab (Transfer Settings Dialog Box)

Getting there

1 Open a VT terminal session and then open the Transfer Settings dialog box.

   The steps depend on your user interface mode (page 216).

User Interface Mode	Steps
Ribbon	On the **Session** ribbon, from the **Transfer** group, click the **Transfer Settings** launcher:
Reflection Browser	On the Reflection menu, choose **Tools** and then **File Transfer**. In the Transfer dialog box, click the **Settings** button.
TouchUx	Tap the Wrench icon and then under **Tools**, select **File Transfer**. In the Transfer dialog box, click the **Settings** button.

2 From the **Transfer Settings** dialog box, select the FTP protocol.

3 Click the **FTP** tab.

The options are:

Log-in options

User name	Enter your user name as it is registered on the FTP server. If you are logging in for the first time, try to log in as **Guest**, or log in by selecting the **Anonymous** check box.

Password	Enter the password the FTP server associates with the user name. When a password is expected and the **Anonymous** check box is selected, the password appears in plain text, instead of asterisks (*), as you type it. If no password is expected, click **OK** to continue.
	For added security, the number of asterisks that show do *NOT* match the number of characters in your password.
	Often, FTP servers expect an e-mail address as a password when you log in as an **Anonymous** user.
Anonymous	Log on to the FTP server as a guest, with the user name `anonymous`.
Enter Host (or System) Name or IP Address	Type the name or IP address of the FTP server to log on to.
Clear Log-in Options	Specify when logon information should be cleared from the controls and fields in this tab (and thus not used as logon information for, as an example, a new host you wish to log on to).
Transfer type	When you perform a file transfer, it defaults to the transfer type you select from this list.

Select	To do this
ASCII	Apply the items under **Translation options for ASCII transfers** (set from the **Translation** tab) to be applied to the file contents, as well as any character set translation that you have opted to perform.
Binary	Transfer the file contents unchanged.
Auto-Detect	Have Reflection select the transfer type for you.

Character set translation (ASCII)	When you perform an ASCII transfer with this option selected, Reflection translates characters based on the settings from the **Translation** tab of the **Transfer Settings**dialog box and the **Emulation** tab of the **Terminal Setup** dialog box.
File name translation	If you are using FTP for ASCII transfers to a host, you can select this option to invoke settings automatically under **File name translation**options on the **Translation**tab.
System type	Select the type of host to which you will send files to or receive files from.
Use passive mode	When selected, the client sends a PASV command to communicate with the server in passive mode (sometimes called *PASV mode*). This initiates a separate data connection for directory listings and file transfers.
	Use passive mode to minimize connection problems with firewalls.

Transfer with	There are two different implementations of FTP available from the **FTP**tab: Reflection FTP and Microsoft FTP.
	Reflection FTP provides connections to any host Reflection supports. Microsoft FTP provides connections to UNIX hosts, and can be used only for FTP transfers to hosts whose FTP server supports UNIX or Windows NT-style server command interfaces.
Default upload directory	Select the host directory to which Reflection should be set after an FTP connection is made. If a directory is listed in this box, the command in the **Host directory command** box is ignored.
Host directory command	Type a host command in this box to retrieve the location of your host's current directory. Reflection uses this information to set the current host directory after an FTP connection is made. The command that's listed can be changed if it does not match your host's "get current host directory" command.
	If a directory is listed in the **Default upload directory** box, that value is used and the command in the **Host directory command** box is ignored.
	NOTE: When **System type** is **Unisys**, only the **Default upload directory** box can be used to set the current host directory.

Related Topics

10 Reflection FTP Client

You can use the FTP Client to transfer files between the local computer and a remote host. The client supports transfers to and from both FTP and SFTP (SSH) servers.

In this Chapter

Introducing Reflection FTP Client

Reflection FTP Client enables you to connect to FTP sites and quickly transfer files using the FTP protocol. It includes the following features:

- A split pane view allows you to browse for both local and server files. **View** menu options allow you to select the display preferences you prefer for viewing files.

- Use standard Windows drag-and-drop and copy-and-paste operations to transfer files between the server and your PC.

- The FTP Client supports a variety of security protocols, including SOCKS, SSL/TLS, Secure Shell, and firewall servers.

- The **FTP Site Wizard** leads you through the steps necessary to configure your FTP site. To launch the wizard, click **New** in the **Connect to FTP Site** dialog box.

- The FTP Client automatically recognizes most common FTP servers. Troubleshooting options for problem servers include support for creating simplified file lists and the **Directory Definition Wizard**.

- An optional command window allows you to view all messages sent between the FTP Client and server. In this view, you can also communicate with the FTP server by entering standard FTP commands directly on a command line.

- Smart file transfer allows FTP client to automatically recognize which transfer method (ASCII or Binary) is appropriate for specified types of files.

- A script recorder allows you to capture actions you take using the FTP Client as command scripts and to play back those scripts to automate connections and file transfers.
- OLE Automation support allows you to script FTP transfers from external applications.

Related Topics

In this Section

Connect to FTP Site Dialog Box

The **Connect to FTP Site** dialog box opens when you start the FTP Client. You can also open it by choosing **Connect** from the **Connection** menu. This dialog box shows all sites that you have defined and saved to the current settings file.

Connect	Connect to the selected site. The client connects using settings you have configured for that site.
New	Add an FTP site. This opens the **Add FTP Site** wizard.
Properties	View or modify the settings for the selected site.
Security	Configure secure connections to the selected site.

Related Topics

View the Local PC Files

To work with items on the local PC, use the left pane of the FTP Client. Commands on the **File** and **Edit** menus, and most buttons on the toolbar, apply to folders and files in the currently active pane.

To view the local PC files

1 Start the FTP Client.

2 Click the left pane to make it active.

3 Use the left pane to browse your files and folders.

NOTE

- To see and navigate the hierarchy of all folders, go to the active pane, click the **Go to a different folder** list box, then choose the folder you want to open.

- To change the way files are displayed, go to the active pane and use the commands on the **View** menu, or use the four view buttons on the toolbar.

Related Topics

- "Managing Files and Folders" on page 815

View the Server Files

To work with items on the server, use the right pane of the FTP Client. Commands on the **File** and **Edit** menus, and most buttons on the toolbar, apply to folders and files in the currently active pane.

To view the server files

1 Start the FTP Client and connect to the remote site.

2 Click the right pane to make it active.

3 To open a folder or file, or to start a program, double-click it.

   To display the contents of a file or run a program, the FTP Client first copies the file from the server to your default local home folder.

NOTE

- For FTP connections (but not SFTP connections) you can use a file view filter to limit the current directory listing to files of a specific type. From the **View** menu, choose **Filter**.

- To see and navigate the hierarchy of all folders, go to the active pane, click the **Go to a different folder** list box, then choose the folder you want to open.

- To change the way files are displayed, go to the active pane and use the commands on the **View** menu, or use the four view buttons on the toolbar.

Related Topics

- "Working with Server Directories" on page 817
- "Filter the Server File Listing" on page 820
- "Set Default Home Directories" on page 818
- "Run the Directory Definition Wizard" on page 821

FTP Client Settings Files

The Reflection FTP Client uses settings files to save your configuration. Settings files include the following information:

- All the sites you have configured, including all site properties. If you have elected to save passwords, these are saved as encrypted text in the settings file.

- Your settings for **Transfer Method** and **If File Exists**.
- Settings that you have configured using the **Options** dialog box.

By default the client automatically opens a settings file named `Settings.rfw` when you start up. You can create shortcuts to launch the client and automatically open any settings file. The client's title bar displays the name of the currently open settings file. Settings files use an RFW file extension.

NOTE

- When you open a settings file, the settings in the file you open replace any currently configured settings.
- You can also use the **Import Settings** command to modify your client settings. When you do, imported settings are appended to any currently configured settings and the title of your session remains unchanged.
- Some display preferences are saved to the Windows registry, not settings files. These settings include your command pane display and your local and server pane view settings. Changes you make to any of these settings affect all client sessions regardless of what settings file is open.
- Prior to version 13.0, settings were saved in the Windows registry. If you have upgraded from an older version your settings are migrated automatically to a settings file the first time you run the client.

Related Topics

-
-
-

Options for Automating FTP Client Transfers

The FTP Client provides the following options for automating file transfers:

- Use FTP Client scripts to automate connections and file transfers from within the client. For details, see and the .
- Use the FTP Client Automation API to automate transfers from external applications. The API documentation is available at http://docs.attachmate.com/reflection/ftp/com-api/.

Connecting to an FTP or SFTP Server

In this Section

-
-
-
-
-

Connect to a Site

You can connect to an FTP or SFTP server in any of these ways:

- ◆ Use the **Connect to FTP Site** dialog box that opens when you launch the client.
- ◆ Create a shortcut that launches a settings file and automatically connects you to a site.
- ◆ Enter an **OPEN** command at the FTP command line. For more information, see the Open topic (page 863) in the Command Reference.
- ◆ Start the client with a startup command that runs a script or connects to a server and performs a file transfer command automatically.
- ◆ Connect to a second site in the same session using **Connect** > **Connect to a Second Site**.

Related Topics

- ◆ "Connect to FTP Site Dialog Box" on page 772
- ◆ "Create a Shortcut to Connect to a Site" on page 825
- ◆ "FTP Client Startup Switches" on page 825
- ◆ "Add a New Site to your Connection List" on page 775
- ◆ "Customizing FTP Client Startup" on page 824
- ◆ "Secure FTP Client Connections" on page 777

Add a New Site to your Connection List

Use the **Connect to FTP Site** dialog box to add new sites to your connection list.

To add a new FTP or SFTP site to your connection list

1 Start the FTP Client.

   This opens the **Connect to FTP Site** dialog box. (If the FTP Client is already running and this dialog box is not open, go to **Connection** > **Connect**.)

2 Click **New** to start the **Add FTP Site Wizard**.

3 Type the host name or IP address of the FTP (or SFTP) server and click **Next**.

4 Specify whether to log in with a user name or using an anonymous login. (Anonymous logons are not allowed for SFTP connections.)

5 (Optional) To configure additional site properties, click **Advanced** in the **Login Information** panel.

6 (Optional) To configure a secure connection, click **Security** in the **Login Information** panel.

   NOTE: You can also modify the security and other properties later. To do this select the site in the **Connect to FTP Site** dialog box and click **Security** or **Properties**.

7 If you are configuring a connection for a registered user, you'll see the **FTP User Login** panel. Type your user name. You can also save your password as obfuscated text in the settings file.

8 In the **Connect** panel, enter a descriptive name for this site. This name is used in the **Connect to FTP Site** dialog box.

9 Specify whether you want to connect to the site now and click **Finish**.

10 From the **File** menu, click **Save** to save this change to the current settings file.

Related Topics

View Connection Information

When you are connected to a host you can display information about the server and the connection.

To view connection information

1 From the **Connection** menu, click **Site Properties**.

2 Click the **Information** tab.

The **Information** tab provides these statistics:

- Some characteristics of the server
- The date and time the connection was opened
- How long the connection has been active
- Duration of the last file transfer operation
- Speed of the last file transfer operation
- Average speed of all file transfer operations during the current session
- Security information about the current session

Preserve a Connection to a Server

Most servers have an "idle time" value that specifies how long a user's session can last when no activity is detected. When the user exceeds the time limit, the server connection is closed. To prevent the server from closing the connection due to inactivity, you can configure the FTP Client to send "keep alive" commands.

To preserve a connection to the server

1 Open the *Site* **Properties** dialog box and then click the **Connection** tab.

2 Select **Send keep alive every <n> seconds** and specify how many seconds to wait in between sending consecutive keep alive (NOOP) commands.

3 Click **OK**.

NOTE: This setting has no effect on SFTP connections. For SFTP connections use **Server Keep Alive** on the **General** tab of the **Secure Shell Settings** dialog box.

Secure FTP Client Connections

The FTP Client supports a variety of security protocols, including SOCKS, SSL/TLS, Secure Shell, and firewall servers.

In this Section

Connect Using a SOCKS Proxy Server

Use this procedure to configure connections in the FTP Client if your site uses a SOCKS proxy server.

To connect using a SOCKS proxy server

1 Start the FTP Client.

   This opens the **Connect to FTP Site** dialog box. (If the FTP Client is already running and this dialog box is not open, go to **Connection** > **Connect**.)

2 Perform one of the following tasks:

To	Do This
Create a new site	From the **Connect to FTP Site** dialog box, click **New**.
	In the **Add FTP Site** dialog box, enter the name or IP address of your FTP server host, and then click **Next**.
	In the **Login Information** dialog box, select **User**.
Modify an existing site	From the **Connect to FTP Site** dialog box, select a site.

3 Click **Security**.

4 SOCKS configuration is different for FTP and SFTP connections:

To	Do this
Configure an FTP connection	On the **SOCKS** tab select **Use SOCKS**. Click **Configure** to configure your SOCKS proxy servers and destination routes.
Configure an SFTP connection	On the **Secure Shell** tab click **Configure** to open the **Reflection Secure Shell Settings** dialog box. On the **General** tab, select **Use SOCKS Proxy**. Click **Configure SOCKS** to configure your SOCKS proxy servers and destination routes.

5 Perform one of the following tasks:

If you are	Do This
Creating a new site	Click **OK** to close the **Security Properties** dialog box and then click **Next**.
	In the **FTP User Login** dialog box, type your user name on the FTP server and then click **Next.**
	Click **Finish**.
Modifying an existing site	Click **OK** to close the open dialog boxes.

NOTE: The default port number for SOCKS servers is 1080.

Connect via a Firewall

Use this procedure if you connect to your FTP or SFTP server through a firewall.

To connect via a firewall

1 Start the FTP Client.

This opens the **Connect to FTP Site** dialog box. (If the FTP Client is already running and this dialog box is not open, go to **Connection** > **Connect**.)

2 Perform one of the following tasks:

To	Do This
Create a new site	From the **Connect to FTP Site** dialog box, click **New**.
	In the **Add FTP Site** dialog box, enter the name or IP address of your FTP server host, and then click **Next**.
	In the **Login Information** dialog box, select **User**.
Modify an existing site	From the **Connect to FTP Site** dialog box, select a site.

3 Click **Security**.

4 On the **Firewall** tab, select **Use Firewall**.

5 Use **Style** to select the authentication command sequence used by your firewall. (The style you select determines which options you can configure in the dialog box.)

6 Configure the appropriate authentication information for your server.

7 Perform one of the following tasks:

If you are	Do This
Creating a new site	Click **OK** to close the **Security Properties** dialog box and then click **Next**.
	In the **FTP User Login** dialog box, type your user name on the FTP server and then click **Next.**
	Click **Finish**.
Modifying an existing site	Click **OK** to close the open dialog boxes.

NOTE

- The **Firewall** tab is not available for SFTP connections.
- The settings in the **Firewall** tab of the Security Properties dialog box are used for all sites that you configure to connect via a firewall.
- When **Use passive mode** is enabled (the default), the FTP Client initiates a separate data connection for directory listings and file transfers. This is required for connections through some firewalls. If passive mode has been turned off and a directory listing does not display or you get an error "425 Can't open data connection," you should enable this setting.

Related Topics

- "Firewall Authentication Styles (FTP Client)" on page 779
- "Connection Tab (Site Properties Dialog Box)" on page 796

Firewall Authentication Styles (FTP Client)

The FTP Client sends different commands for logging onto a firewall and connecting to an FTP server based on the style of server you specify. During this authentication sequence, the FTP Client uses information you have configured in the *Site* > **Properties** dialog box and the **Firewall** tab of the **Security Properties** dialog box. If you have not configured all or part of this information, you'll be prompted for it each time you make a connection.

The following styles are available:

SITE servername

Use this style if your passthrough server sends a SITE command to connect to the FTP server. For details, see the "SITE Servername Authentication Command Sequence" on page 780.

username@servername

Use this style if your passthrough server requires server logon information in the format `username@servername`. For details, see the "Username@servername Authentication Command Sequence" on page 781.

USER-PASS-ACCT

Use this style when you don't need to specify a proxy server because your network automatically routes connections through the firewall. In this logon sequence both the FTP site and firewall user names are sent with a single USER command and the firewall password is sent with the ACCT command. For details, see the "USER-PASS-ACCT Authentication Command Sequence" on page 781.

Transparent

Use this style when you don't need to specify a proxy server because your network automatically routes connections through the firewall. In connections made using this style, a sequence of USER and PASS commands sends logon information for the firewall followed by the FTP server. For details, see the "Transparent Authentication Command Sequence" on page 781.

Challenge/Response

Use this style if your server requires you to use a hardware token to enter identification information when you open a connection. When you select this style, you can't preconfigure password information. During the login process, you'll see a challenge prompt. Use your token to determine the correct information to enter in response to this prompt. For details, see the "Challenge/Response Authentication Command Sequence" on page 782.

UserID@FireID@RemoteHost

Use this style if your server requires a login of the style UserID@FireID@RemoteHost. If you leave the other boxes blank, the FTP Client prompts for information in this order when you make a connection: Firewall address, Firewall user name, Firewall password, FTP server address, FTP user name.

FirewallUser@FTPServer

Use this style if your server requires a login of the style FirewallUser@FTPServer. If you leave the other boxes blank, the FTP Client prompts for information in this order when you make a connection: Firewall address, Firewall username, Firewall password and FTP username. For details, see "FirewallUser@FTPServer Authentication Command Sequence" on page 782.

FtpUser@FtpServer FirewallUser

Use this style if your server requires a login of the style FtpUser@FtpServer FirewallUser. If you leave the other boxes blank, the FTP Client prompts for information in this order when you make a connection: Firewall address, Firewall username, Firewall password, FTP user name FTP password. For details, see "FTPUser@FTPServer FirewallUser Authentication Command Sequence" on page 782.

Related Topics

- "Connect via a Firewall" on page 778

SITE Servername Authentication Command Sequence

The FTP Client uses the following command sequence to make a connection when you have configured **Style** to **SITE servername** in the **Firewall** tab of the **Security Properties** dialog box.

```
OPEN <proxy_server>
USER <firewall_username>
PASS <firewall_password>
SITE <FTP_server>
USER <FTP_server_username>
PASS <FTP_server_password>
```

Related Topics

- "Connect via a Firewall" on page 778

Username@servername Authentication Command Sequence

The FTP Client uses one of the following command sequences to make a connection when you have configured **Style** to **username@servername** in the **Firewall** tab of the **Security Properties** dialog box.

When **Passthrough authentication** is selected:

```
OPEN <proxy_server>
USER <firewall_username>
PASS <firewall_password>
USER <username>@<FTP_server>
PASS <FTP_server_password>
```

When **Passthrough authentication** is not selected:

```
OPEN <proxy_server>
USER <username>@<FTP_server>
PASS <FTP_server_password>
```

Related Topics

- "Connect via a Firewall" on page 778

USER-PASS-ACCT Authentication Command Sequence

The FTP Client uses the following command sequence to make a connection when you have configured **Style** to **USER-PASS-ACCT** in the **Firewall tab** of the **Security Properties** dialog box.

```
OPEN <FTP_server>
USER <FTP_server_username> <firewall_username>
PASS <FTP_server_password>
ACCT <firewall_password>
```

Related Topics

- "Connect via a Firewall" on page 778

Transparent Authentication Command Sequence

The FTP Client uses the following command sequence to make a connection when you have configured **Style** to **Transparent** in the **Firewall tab** of the **Security Properties** dialog box.

```
OPEN <FTP_server>
USER <firewall_username>
PASS <firewall_password>
USER <FTP_server_username>
PASS <FTP_server_password>
```

Related Topics

* "Connect via a Firewall" on page 778

Challenge/Response Authentication Command Sequence

The FTP Client uses the following command sequence to make a connection when you have
configured **Style** to **Challenge/Response** in the **Firewall** tab of the **Security Properties** dialog box.

```
OPEN <FTP_server>
USER <firewall_username>
PASS <challenge_response_from_token>
USER <FTP_server_username>
PASS <FTP_server_password>
```

Related Topics

* "Connect via a Firewall" on page 778

FirewallUser@FTPServer Authentication Command Sequence

The FTP Client uses the following command sequence to make a connection when you have
configured **Style** to **FirewallUser@FTPServer** in the **Firewall** tab of the **Security Properties** dialog box.

```
OPEN <Firewall_server>
USER <Firewall_username>@<FTP_server>
PASS <Firewall_password>
USER <FTP_username>
```

Related Topics

* "Connect via a Firewall" on page 778

FTPUser@FTPServer FirewallUser Authentication Command Sequence

The FTP Client uses the following command sequence to make a connection when you have
configured **Style** to **FTPUser@FTPServer FirewallUser** in the **Firewall** tab of the **Security Properties**
dialog box.

```
OPEN <Firewall_server>
USER <FTP_username>@<FTP_server> <Firewall_username>
PASS <FTP_server_password>
ACCT <Firewall_password>
```

Related Topics

* "Connect via a Firewall" on page 778

Secure Shell Connections (FTP Client)

Secure Shell connections require both server and user authentication. The Secure Shell protocol also provides data encryption. When you configure Secure Shell connections in the FTP Client, you can use either of the following approaches to ensure that all transferred data is securely encrypted.

- Transfer files using the SFTP protocol.
- Transfer files using the FTP protocol and use tunneling to forward all communications through the secure SSH tunnel.

Related Topics

- "Connect Using Secure Shell (FTP Client)" on page 783
- "Forward FTP communications" on page 784

Connect Using Secure Shell (FTP Client)

The following procedure describes how to use Secure Shell for authentication and encryption in the FTP Client.

To configure secure Shell connections in the FTP Client

1 Start the FTP Client.

   This opens the **Connect to FTP Site** dialog box. (If the FTP Client is already running and this dialog box is not open, go to **Connection** > **Connect**.)

2 Perform one of the following tasks:

To	Do This
Create a new site	From the **Connect to FTP Site** dialog box, click **New**.
	In the **Add FTP Site** dialog box, enter the name or IP address of your FTP server host, and then click **Next**.
	In the **Login Information** dialog box, select **User**.
Modify an existing site	From the **Connect to FTP Site** dialog box, select a site.

3 Click **Security**.

4 Click the **Secure Shell** tab.

5 Select **Use Reflection Secure Shell**.

6 Select one of the following options:

SFTP	Reflection will connect using SFTP (Secure FTP) protocol. SFTP supports fewer commands than the full FTP protocol.
Tunnel FTP using port forwarding	Reflection will secure the port you specify for **Local port** through the SSH tunnel. With this configuration you have access to the full range of FTP commands. All communications are sent through the SSH tunnel. This includes FTP commands (including user name and password) and all transmitted data (including directory listings and the contents of the files you transfer)

7 (Optional) Specify an **SSH config scheme**. (If you leave **SSH config scheme** blank, Reflection saves any changes you make to an SSH configuration scheme with the same name as the current host.)

8 (Optional) Click **Configure** to open the **Reflection Secure Shell Settings** dialog box. Use this dialog box to configure user authentication and additional Secure Shell settings.

9 Perform one of the following tasks:

If you are	Do This
Creating a new site	Click **OK** to close the **Security Properties** dialog box and then click **Next**.
	In the **FTP User Login** dialog box, type your user name on the FTP server and then click **Next.**
	Click **Finish**.
Modifying an existing site	Click **OK** to close the open dialog boxes.

NOTE

  ◆ Host authentication enables the Secure Shell client to reliably confirm the identity of the Secure Shell server. This authentication is done using public key authentication. If the host public key has not previously been installed on the client, the first time you attempt to connect you see a message indicating that this is an unknown host. This message includes a fingerprint that identifies the host. To be sure that this is actually your host, you should contact the host system administrator who can confirm that this is the correct fingerprint. Until you know that the host is actually your host, you are at risk of a "man-in-the-middle" attack, in which another server poses as your host.

  ◆ In most cases you will be able to connect to your host and log in with your password using the default Secure Shell configuration. Use the **Reflection Secure Shell Settings** dialog box if you need to configure alternate user authentication methods or to make other changes to your Secure Shell configuration.

  ◆ The default **Server Type** setting for the FTP Client is **Auto detect**. This setting is not valid when Secure Shell is configured for SFTP. The FTP Client will automatically modify this setting from **Auto detect** to **UNIX** when you configure Secure Shell to use SFTP. To change to a different server type, use the **General** tab of the *Site > Properties* dialog box after you configure the Secure Shell settings.

Related Topics

  ◆ "Secure Shell Connections (FTP Client)" on page 783

Forward FTP communications

Use this procedure to encrypt FTP protocol communications (including the FTP command channel and all data channels) using Secure Shell port forwarding. By using port forwarding, you can make secure connections to FTP servers and have access to the full range of FTP options and commands, including some that are not available with SFTP connections.

NOTE: To enable forwarding of the data channel(s), the FTP Client must be configured to communicate in passive (PASV) mode (the default).

To forward FTP communications

1 Start the FTP Client.

   This opens the **Connect to FTP Site** dialog box. (If the FTP Client is already running and this dialog box is not open, go to **Connection** > **Connect**.)

2 Perform one of the following tasks:

To	Do This
Create a new site	From the **Connect to FTP Site** dialog box, click **New**.
	In the **Add FTP Site** dialog box, enter the name or IP address of your FTP server host, and then click **Next**.
	In the **Login Information** dialog box, select **User**.
Modify an existing site	From the **Connect to FTP Site** dialog box, select a site.

3 Click **Security**.

4 Click the **Secure Shell** tab.

5 Select **Use Reflection Secure Shell**.

6 Select **Tunnel FTP using port forwarding**

7 This step is required only if your Secure Shell server is on a different host than the FTP server.

   ◆ Select **FTP host is different than Secure Shell host**.

   NOTE: When you select **FTP host is different than Secure Shell host**, FTP commands and data are transmitted securely from your client computer to the Secure Shell server through a secure tunnel. The commands and data are transmitted in the clear between the Secure Shell server and the FTP server.

   ◆ For **SSH server address,** type your Secure Shell server host name or IP address.

   ◆ For **SSH user name**, type your login name on the Secure Shell server.

8 Perform one of the following tasks:

If you are	Do This
Creating a new site	Click **OK** to close the **Security Properties** dialog box and then click **Next**.
	In the **FTP User Login** dialog box, type your user name on the FTP server and then click **Next.**
	Click **Finish**.
Modifying an existing site	Click **OK** to close the open dialog boxes.

NOTE: You will need to authenticate to both the Secure Shell server and the FTP server.

SSL/TLS Connections (FTP Client)

The Secure Sockets Layer protocol (SSL) and its compatible successor, the Transport Layer Security protocol (TLS), enable a client and server to establish a secure, encrypted connection over a public network. When you connect using SSL/TLS, the client authenticates the server before making a connection, and all data passed between the client and the server is encrypted. Depending on the server configuration, the server may also authenticate the client.

Configure SSL/TLS (FTP Client)

NOTE: SSL/TLS connections use digital certificates for authentication. Depending on how your certificate was issued and the way your host is configured, you may need to install a host and/or personal certificate before you can connect using SSL/TLS.

To configure a secure SSL/TLS connection in the FTP Client

1 Start the FTP Client.

This opens the **Connect to FTP Site** dialog box. (If the FTP Client is already running and this dialog box is not open, go to **Connection** > **Connect**.)

2 Perform one of the following tasks:

To	Do This
Create a new site	From the **Connect to FTP Site** dialog box, click **New**.
	In the **Add FTP Site** dialog box, enter the name or IP address of your FTP server host, and then click **Next**.
	In the **Login Information** dialog box, select **User**.
Modify an existing site	From the **Connect to FTP Site** dialog box, select a site.

3 Click **Security**.

4 From the **SSL/TLS** side menu, select **Use SSL/TLS Security**.

5 (Optional) To specify the minimum allowable level of encryption for SSL/TLS connections, select a level in the **Encryption strength** list. The connection fails if this level cannot be provided.

Encryption strength options	Description
Recommended ciphers	When Recommended ciphers is selected, the FTP Client will negotiate with the host system to choose the strongest encryption level supported by both the host and the client. This new setting will contain the recommended encryption level from Micro Focus, and will change periodically.
	If you are running in FIPS mode and select Recommended ciphers, the FTP Client will negotiate using only FIPS compliant encryption levels.
Custom ciphers	When Custom ciphers is selected, you will be prompted to select from a list of available ciphers in the Custom Ciphers list view.
	NOTE: Session files from previous versions of Reflection that use default, 168, 128 or 256 bit Encryption Strength will be imported as Custom ciphers and maintain the list that was used in prior versions for those settings options.

6 (Optional) Click **Configure PKI**.

The **PKI Configuration** dialog box opens, from which you can manage the digital certificates used for authentication.

6a Click **Reflection Certificate Manager**.

6b In the Reflection Certificate Manager dialog box, select the **Trusted Certificate Authorities** tab.

6c Click **Import** and browse to select the CA certificate for the server.

6d Modify default settings as required. (For example, to use only the Reflection Certificate Manager, you might choose to clear **Use System Certificate Store for SSL/TLS connections**. When this option is selected, Reflection FTP Client looks for certificates in both the Reflection Certificate Manager store and the Windows certificate store.)

When you customize any of the default PKI settings, the `pki_config` file is created.

6e Close the Certificate Manager dialog box and click **OK** to close the other open dialog boxes.

The imported certificate is saved in the `trust_store.p12` file.

6f After a connection is established, click the Save button on the Quick Access toolbar and save the session document.

7 Perform one of the following tasks:

If you are	Do This
Creating a new site	Click **OK** to close the **Security Properties** dialog box and then click **Next**.
	In the **FTP User Login** dialog box, type your user name on the FTP server and then click **Next.**
	Click **Finish**.
Modifying an existing site	Click **OK** to close the open dialog boxes.

NOTE

- Before making an SSL/TLS connection, Reflection authenticates the host system. The certificate presented by the host for this purpose must be from a trusted certificate authority. If your computer does not recognize the certificate authority, you will not be able to make SSL/TLS connections. Depending on how a host certificate was issued, you may need to install the certificate on your computer.

- When you make an SSL/TLS connection, a padlock icon appears indicates that the data stream is encrypted. A key icon indicates that the command channel (including the entered password) is encrypted

Working with FTP Client Settings Files

The Reflection FTP Client uses settings files to save your configuration. Settings files use an RFW file extension.

In this Section

- "Save your FTP Client Settings" on page 788
- "Load Saved FTP Client Settings" on page 789
- "Import FTP Client Settings" on page 789
- "Import WS_FTP Settings into FTP Client" on page 790
- "Save Changes on Exit Dialog Box" on page 790
- "Export FTP Settings Dialog Box" on page 791

Related Topics

- "FTP Client Settings Files" on page 773

Save your FTP Client Settings

When you start the FTP Client from the Windows **Start** menu, the client automatically opens a settings file named `Settings.rfw` and any changes you make to your configuration are saved to this file. If you choose, you can also create additional settings files.

To save your settings to the currently open settings file

♦ From the **File** menu, choose **Save**.

To save your settings to a different settings file

1 From the **File** menu, select **Save As**.

2 Type a name for the file you are saving.

3 (Optional) Select **Save shortcut on desktop** if you want to save a shortcut to your desktop that will launch the client and open the settings file you are saving.

4 Click **Save**.

Related Topics

♦ "FTP Client Settings Files" on page 773

♦ "Load Saved FTP Client Settings" on page 789

♦ "Import FTP Client Settings" on page 789

♦ "Create a Shortcut to Load a Settings File" on page 824

Load Saved FTP Client Settings

When you start the FTP Client from the Windows **Start** menu, the client automatically opens a settings file named `Settings.rfw` and any changes you make to your configuration are saved to this file. If you have created additional settings files, you can use either of these techniques to open them.

To open a settings file from the FTP Client

♦ From the **File** menu, choose **Open** and then browse to locate your saved file.

To open a settings file using a Windows shortcut

1 When you save your settings file, create a shortcut to it.

2 Use this shortcut to launch the client and load that settings file.

Related Topics

♦ "Save your FTP Client Settings" on page 788

♦ "Create a Shortcut to Load a Settings File" on page 824

♦ "Import FTP Client Settings" on page 789

♦ "FTP Client Settings Files" on page 773

Import FTP Client Settings

You can export FTP Client settings to XML format using the **Export Settings** command. This procedure imports settings from an XML file.

To import settings from an XML file

1 From the **File** menu, choose **Import Settings**.

2 Browse to locate the XML file that contains your site configuration.

3 Click **Open**.

You will see a message telling you that the sites were imported successfully.

4 Click **OK**.

NOTE: Settings in the imported file are appended to any currently configured settings, and your session title is not changed. This is different from opening a saved settings file (*.rfw). When you open a settings file, the settings in that file replace any currently configured settings in the client, and your session title changes to the name of the open settings file.

Related Topics

- "Save your FTP Client Settings" on page 788
- "Load Saved FTP Client Settings" on page 789
- "FTP Client Settings Files" on page 773
- "Export FTP Settings Dialog Box" on page 791

Import WS_FTP Settings into FTP Client

If you are migrating from WS_FTP, you can import your settings into FTP Client.

Before you begin, locate your `wsftp_options.ini` file, typically in the following location:

`C:\Users\<user>\AppData\Roaming\IPSwitch\WS_FTP`

To import WS_FTP settings

1 From the FTP Client **File** menu, choose **Import Settings**.

2 From the **Files of type** drop-down list, select "Import WS_FTP (wsftp_options.ini)."

3 Browse to locate your `wsftp_options.ini` file, click **Open**, then click **OK**.

4 You should see a message saying that your settings were imported successfully.

5 Click **File**> **Save** to save the imported settings.

Related Topics

- "Save your FTP Client Settings" on page 788

Save Changes on Exit Dialog Box

Reflection FTP Client displays the **Save Changes on Exit** dialog box if you have made any changes to your settings in the current session. The options are:

Save	Saves all changes you have made to settings.
Discard	Exits without saving any changes you have made during the current session.
Cancel	Cancels the exit command and returns you to the Reflection session without saving any changes.

Export FTP Settings Dialog Box

Getting there

 ◆ From the FTP Client **File** menu, choose **Export Settings**.

The options are:

Sites	Site-specific settings are configured using the *Site* > **Properties** dialog box or the **Directory Definition Wizard**. All settings are exported for each site with the exception of user name and password, which are included only when **User Settings** is also selected.
	Select which of your currently configured sites are included in the exported settings file. Select a site and click **Remove** if you don't want the site included in the exported file.
Application Settings	Application settings affect the behavior of the FTP Client and are independent of both site and user. The following information is included:
	◆ **Options** dialog box, **General** tab - **Default local home folder**
	◆ **Options** dialog box, **File Types** tab - All features
	◆ **Options** dialog box, **Preferences** tab - All features
User Settings	The following information is included:
	◆ *Site* **Properties** dialog box - **User** and **Password**
	◆ **Options** dialog box, General tab - **Anonymous password**
	◆ Custom rules created using the **Directory Definition Wizard**.
File Name	Type a path and filename for the exported settings file. If you change the default filename, you must include a file extension if you wish to use one.

Related Topics

Configuring Site and Global Properties

In this Section

Change Global Settings for the FTP Client

Global settings allow you to configure the default behavior for connections to all servers.

To configure global settings

1 From the **Tools** menu, choose **Options**.

Related Topics

General Tab (Options Dialog Box)

Getting There

- From the FTP Client **Tools** menu, choose **Options**.

The options are:

Anonymous Password	Type the default password to use for anonymous connections to FTP sites.
	This feature is not available for SFTP connections.
Default local home folder	Specify the folder that displays automatically when you start the client and receives files transferred from the server. Your Windows user folder is the default.
	Default local home folder is a global default. It is ignored if you specify a site-specific value for **Home folder** on the **Directories** tab in the *Site > Properties*dialog box.
	You can specify a local home folder using UNC paths such as:
	`\\<computername>\<sharename>\<pathname>`

Related Topics

File Types Tab (Options Dialog Box)

Getting There

- From the FTP Client **Tools** menu, choose **Options**.

Use this tab to configure Smart file transfer. When Smart file transfer is enabled, any file of a defined file type is transferred using the transfer method specified for that file type. To enable Smart file transfer, go to **Tools** > **Transfer Method** > **Smart**.

The options are:

Smart file transfer types	Lists all file types that have been assigned a transfer method.
New	Open the **Add Smart File Type** dialog box.
Delete	Remove the currently selected file type from the list.
Change	Edit the currently selected file type.
Transfer method for undefined file types	Specify a default for files types that have no associated transfer method.
	If **Ask User** is specified, you are prompted to specify a transfer method when you transfer a file with that extension. At that time you can select a specific transfer method or choose **Always ask user**.

Related Topics

Preferences Tab (Options Dialog Box)

Getting There

- From the FTP Client **Tools** menu, choose **Options**.

The options are:

When the FTP Client exits	Select how the client handles configuration changes. If you select **Save configuration automatically**, changes are saved to the current settings file.
Confirm file delete	Select whether the client prompts you for confirmation before deleting a file or folder.
Hide progress window	Suppress the connection progress, transfer progress, and error notification dialog boxes.
Do not use animation	By default Reflection uses animation during certain actions, for example a waving flashlight appears while you are waiting for a directory listing. Turning off the use of animation may fix some problems that cause Reflection to become unresponsive.
Force site-to-site transfers through local machine	Force all site-to-site transfers to copy files first to the local computer then to the destination server. Use this for FTP servers that don't support direct site-to-site transfers.
	NOTE: If there is a secure connection to either server, or the transfer type is not **Binary**, the client always transfers files this way, regardless of the value of this setting.

Related Topics

File Attributes Tab (Options Dialog Box)

Getting There

- From the FTP Client **Tools** menu, choose **Options**.

Use this tab to configure default attributes for file transfers.

Set default file attributes on uploads	Set default permissions for files copied to the server. When **Set default file attributes on uploads** is selected, you can specify permissions using either the **Permission Mode** box, or using the **Owner**, **Group**, and **Public** check boxes. **NOTE** • To specify non-default permissions during a file transfer, you can configure **Site Properties** > **Transfer** > **Show upload options before transfer**. When this setting is enabled, the **File Upload Options** dialog box is displayed before you transfer files to the server. • When **Set default file attributes on uploads** is selected, the client sends a **chmod** command to the server to set the permissions you have specified. If your server does not support this command, you will receive a server error message that the **chmod** command is unrecognized.
Set default file attributes on downloads	Set default attributes for files copied to the client. When **Set default file attributes on downloads** is selected, you can specify attributes using the Read-only and/or Hidden check boxes. **NOTE:** To specify non-default permissions during a file transfer, you can configure **Site Properties** > **Transfer** > **Show download options before transfer**. When this setting is enabled, the **File Download Options** dialog box is displayed before you transfer files to the client.

Related Topics

Change Settings for an FTP or SFTP Site

Use the **Site Properties** dialog box to configure how the client behaves when connecting and interacting with a particular remote site.

To modify the settings for a particular site

1 Start the FTP Client.

   This opens the **Connect to FTP Site** dialog box. (If the FTP Client is already running and this dialog box is not open, go to **Connection** > **Connect**.)

2 From the **Connect to FTP Site** dialog box, select a site.

3 Click the **Properties** button.

NOTE

  ◆ If you are already connected to a site, from the **Connection** menu, choose **Site Properties**.

  ◆ Some changes you make using the **Site > Properties** dialog box when connected will not take effect until the next time you connect to the site.

Related Topics

  ◆ "General Tab (Site Properties Dialog Box)" on page 795

  ◆ "Connection Tab (Site Properties Dialog Box)" on page 796

  ◆ "Directories Tab (Site Properties Dialog Box)" on page 798

  ◆ "Translation Tab (Site Properties Dialog Box)" on page 800

  ◆ "Transfer Tab (Site Properties Dialog Box)" on page 801

  ◆ "Information Tab (Site Properties Dialog Box)" on page 804

  ◆ "Change Global Settings for the FTP Client" on page 791

General Tab (Site Properties Dialog Box)

Getting there

1 Start the FTP Client.

This opens the **Connect to FTP Site** dialog box. (If the FTP Client is already running and this dialog box is not open, go to **Connection** > **Connect**.)

2 From the **Connect to FTP Site** dialog box, select a site.

3 Click the **Properties** button.

NOTE

  ◆ If you are already connected to a site, from the **Connection** menu, choose **Site Properties**.

  ◆ Some changes you make using the **Site > Properties** dialog box when connected will not take effect until the next time you connect to the site.

Use this tab to provide connection information for the specified site.

The options are:

FTP address	Type the FTP or SFTP server to log on to. This can be a domain name, a URL, or an IP address.
Server type	In most cases, FTP Client will correctly identify your server when this value is set to **Auto detect**. If FTP Client is not successfully identifying the type of server you are connecting to, select it from this list. **Auto detect** is not available for SFTP sessions. The default for these sessions is **UNIX**.

Log on as

Anonymous	Log on to the FTP server as a guest, with the user name `anonymous`. (Anonymous logons are not allowed for SFTP connections.)
	If you log on to this server anonymously, the **Password** box is automatically filled in with the anonymous password specified on the **General** tab in the **Options** dialog box. If this FTP site expects a different password for anonymous users, type the site-specific password here.
User	Log on to the specified server using a registered user name.
User name	Enter your user name as it is registered on the FTP server.
Save password as obfuscated test	Save your password as obfuscated text in your settings file and use it to log on to this server.
Password	Enter the password the FTP server associates with the user name registered on the FTP server.
Use Windows Credentials	Use your Windows credentials instead of your FTP user name and password when performing a data transfer.
	NOTE: This option can be used only with IBM System i (AS/400) and IBM AS/400 (Format 0) server types.
Security	Configure a secure connection to the specified server.

Connection Tab (Site Properties Dialog Box)

Getting there

1 Start the FTP Client.

This opens the **Connect to FTP Site** dialog box. (If the FTP Client is already running and this dialog box is not open, go to **Connection** > **Connect**.)

2 From the **Connect to FTP Site** dialog box, select a site.

3 Click the **Properties** button.

NOTE

  ◆ If you are already connected to a site, from the **Connection** menu, choose **Site Properties**.

  ◆ Some changes you make using the **Site > Properties** dialog box when connected will not take effect until the next time you connect to the site.

Use this tab to configure settings for maintaining connections and to set timeout intervals.

NOTE: For SFTP connections, the only setting available from this tab is **Use IPV6**.

Connection options

Use passive mode
When selected, the client sends a PASV command to communicate with the server in passive mode (sometimes called *PASV mode*). This initiates a separate data connection for directory listings and file transfers.

Use passive mode to minimize connection problems with firewalls.

If passive mode has been turned off and a directory listing does not display or you get an error "425 Can't open data connection," you should enable this setting.

IPV6 connections use EPSV.

Send keep alive every \<n\> seconds
Most FTP servers have an "idle time" value that specifies how long a user's FTP session can last when no activity is detected. When the user exceeds the time limit, the server connection is closed. This setting allows you to direct the Client to send a NOOP command to the server at timed intervals to prevent the server from closing the connection due to inactivity. When selected, specify the number of seconds to wait between transmissions of NOOP commands.

TCP port
Use the **TCP port** box to specify a non-standard TCP service port number or socket for FTP. The default value **21** is the standard service port for FTP.

Account
If your server requires an account name for file access, type it here. For case-sensitive servers, be sure to use the appropriate case.

When a connection is opened, if **Account** is filled in, the client automatically sends the account name to the server as the last logon step.

Timeouts in seconds

Connect
Select the maximum number of seconds to continue trying to establish an FTP server connection. Entering 0 (zero) in this box prevents the FTP Client from ever timing out on a connection attempt.

Session
Select the maximum number of seconds to wait for data packets being transferred to or from the host. If nothing is received within the period specified, a timeout error displays and the transfer is aborted; in this case, try the operation again. If you receive repeated timeout errors, increase the timeout value. Entering 0 (zero) in this box prevents the FTP Client from ever timing out when waiting for a response.

Other settings

Use IPV6
Select whether connections to the host use IPV6 (Internet Protocol version 6) or the older IPv4 protocol. By default, the client attempts to connect using IPv6, and uses IPv4 when IPv6 is not available. You may need to change this value to "Never" if you are having problems connecting to hosts on an IPv4 network from a client computer with IPv6 enabled.

Initial umask	Use this setting to specify an initial umask value to send to the server upon connection. You can use umask to modify the default permissions attributes set on newly created files. When you specify a umask, the client sends the following to the FTP server when you login, where nnnn is your specified umask value.

`SITE umask `*nnnn*

To find out if umask is a supported SITE command for your FTP server, enter this command at the FTP command line:

`QUOTE help site`

NOTE

- ◆ The umask set by the FTP client cannot be less restrictive than user permissions set on the server.

- ◆ This option is not available if you have configured global upload attributes using **Tools**> **Options**> **Attributes**> **Set default attributes on uploads**.

- ◆ This option is not available for SFTP connections.

Directories Tab (Site Properties Dialog Box)

Getting there

1 Start the FTP Client.

This opens the **Connect to FTP Site** dialog box. (If the FTP Client is already running and this dialog box is not open, go to **Connection** > **Connect**.)

2 From the **Connect to FTP Site** dialog box, select a site.

3 Click the **Properties** button.

NOTE

- ◆ If you are already connected to a site, from the **Connection** menu, choose **Site Properties**.

- ◆ Some changes you make using the **Site > Properties** dialog box when connected will not take effect until the next time you connect to the site.

Use this tab to specify how your directory listings are displayed. The options are:

Server

Home directory	Select the server directory the FTP Client should display after a connection is made.
Show directory upon connection	Select whether a list of the files and folders in the working server directory is displayed in the right pane each time you open a connection to this site. If you choose not to show server directories and you want to change to a different server directory, use the **Go To** command on the **Tools** menu or use the "CD" on page 885 command at the FTP command line.

Refresh directory automatically	Select whether the server directory listing shown in the right pane is updated when you execute a "CD" on page 885 command, or perform any operation that adds or deletes files or directories on the server.
Try to convert dates to local system format	Select whether dates display in the format specified by the regional settings in Windows Control Panel. Leave this check box cleared if you want dates to display in the date format used on the server.
Resolve links	Select how directory listings are created when you are connected to a server that supports symbolic links. When this box is checked, the server pane correctly uses folders to display symbolic links that identify directories. Clear this box if you don't need this feature and you want to improve response time for new or refreshed file listings.
Cache directory listing	Select whether directory listings are cached on your local PC. Using cached directory listings speeds up the server pane display as you navigate through your server directories, but will not reflect changes you have made to your server files. When this box is cleared, file listings are updated from the server each time you change the display.
	NOTE: Using the **Refresh** command (F5) always shows any changes you have made on the server even if you are using cached file listings.
Display file names only	Select whether directory listings include filenames only. You can use this setting as a troubleshooting tool if the client is having difficulty displaying directory listings for your host. When this check box is cleared, file listings are created using the FTP LIST command; when it is selected, file listings use NLST.
	This setting does not apply to SFTP connections.
Don't send PWD command	When this option is selected, the FTP Client does not send a PWD command when you are connected to the server. Enabling this setting may fix connection problems encountered with some hosts. When it is enabled, the current server directory path won't be displayed in the server's title bar, and the **Go to a different Folder** list box (located on the left side of the toolbar), will not display host directory information. You will see your local PC directories even when the server pane is selected.
	NOTE: Press F7 to open the command window before you try connecting to your server. If the server returns an error after Reflection sends the PWD command, try enabling this setting.
	This setting does not apply to SFTP connections.
File View Filter	Type a default file view filter for the server using wildcard characters that are recognized by the server. For more information, see the "Filter the Server File Listing" on page 820 topic.
	This feature is not available for SFTP connections.

LIST command parameters	Specify the command parameters the FTP Client uses when it sends an FTP LIST command to the server. The appropriate parameters depend on the type of server you are connecting to. Changing this value may help troubleshoot some problems. Use caution when modifying LIST command parameters for use with the "MDEL" on page 860 command.
	On some systems the list can be set to recursively list files in subfolders.
	This feature is not available for SFTP connections.
Show attributes before creating directory	Select this option to see a dialog box that enables you to set directory permissions whenever you create a new directory on the server.

Local

Home folder	Type the path to a home (default) folder for the FTP Client. When a connection to the site is opened, the local working folder is set automatically to the specified home path and that location will receive any server files you transfer using the **Download** command.
	The global **Default local home** folder setting is ignored for this site.

Related Topics

- "Filter the Server File Listing" on page 820

Translation Tab (Site Properties Dialog Box)

Getting there

1 Start the FTP Client.

This opens the **Connect to FTP Site** dialog box. (If the FTP Client is already running and this dialog box is not open, go to **Connection** > **Connect**.)

2 From the **Connect to FTP Site** dialog box, select a site.

3 Click the **Properties** button.

NOTE

- If you are already connected to a site, from the **Connection** menu, choose **Site Properties**.

- Some changes you make using the **Site > Properties** dialog box when connected will not take effect until the next time you connect to the site.

Use this tab to control conversion of formatting characters in ASCII data transferred to the client or to the server.

NOTE: **Translation** tab settings are not available for SFTP connections.

To server

Change tabs to spaces	Spaces replace tab characters in uploaded files.
Spaces per tab	Define the size of the tab stops used if you change spaces to tabs or tabs to spaces.
Read CTRL-Z as end of file	When selected, file transfer uses a Ctrl-Z (^Z) character as the end-of-file marker, and strips it from the file being sent. Otherwise, the character count in the file directory is used to determine the file length. The FTP Client never sends Ctrl-Z if it is the last character in an ASCII file.

From server

Change spaces to tabs	Select to have tab characters replace consecutive spaces in downloaded files. Use **Spaces per tab** (under **To server**) to specify how many spaces equal one tab.
Write Ctrl-Z at end of file	On the local computer, ASCII text files normally end with a Ctrl-Z (^Z) character. If you want a ^Z character added to the file when it is received from the server, keep this option selected. Some Windows applications require this marker.
Delete trailing spaces	Select to save local disk space. Some host text files use fixed-length records to delimit lines; they pad the end of each record with blanks. Most PC text processing programs use a carriage return and linefeed sequence to delimit lines and paragraphs, and thus do not need blanks preceding a delimiter.
A six digit date on the server represents	Select how six digit dates on the server are interpreted. **MM** represents the month, **DD** the day, and **YY** the year.

Additional options

Character Sets button	Open the **Character Sets** dialog box to configure translation between the server character set and either the Windows or DOS character set.

Related Topics

- "Character Sets Dialog Box" on page 812

Transfer Tab (Site Properties Dialog Box)

Getting there

1 Start the FTP Client.

   This opens the **Connect to FTP Site** dialog box. (If the FTP Client is already running and this dialog box is not open, go to **Connection** > **Connect**.)

2 From the **Connect to FTP Site** dialog box, select a site.

3 Click the **Properties** button.

NOTE

- If you are already connected to a site, from the **Connection** menu, choose **Site Properties**.
- Some changes you make using the **Site > Properties** dialog box when connected will not take effect until the next time you connect to the site.

Use this tab to specify how filenames and dates are handled during file transfers to and from the server. The options are:

Download from server options

Preserve server file date	Retain the original date stamps associated with downloaded files. If you want files transferred from the server to be date stamped with the time and date when they were transferred, keep this check box cleared. **NOTE:** Server file dates will not be preserved if the **Display file names only** setting on the **Directories** tab has been enabled. Server file dates are not preserved when files are dragged to the Windows desktop or Windows Explorer folder. Drag files to the local pane of the FTP Client to preserve file dates. To retain original server dates in transfers done by a script, you can either load your site settings when you launch the script (page 827) or add the following line to the beginning of the script: `PRESERVE-FILE-DATE yes`
Create Windows file names in 8.3 format	Select to receive host files in the DOS 8.3 filename format. For example, a file with the name `Longfilename.Document` will be converted automatically to `Longfile.doc` when transferred to your PC. **NOTE:** During wildcard transfers with this check box selected, if two long filenames translate to the same DOS 8.3 format name, the second file transferred will overwrite the first when **If File Exists** is set to **Overwrite**.To prevent this, change the **If File Exists** setting to **Unique**.
Try to resume partial binary downloads	Select to have the FTP Client try to resume downloading the untransferred portion of files after an interruption. For more information, see the "Resume an Incomplete Server File Download" on page 810 topic. This feature is not available for SFTP connections.
Show download options before transfer	Select this option if you want to be queried for the transfer method (for example, ASCII or binary) and file properties (read-only or hidden) before downloading a new file from the server.
Send SITE command before transfer	Type a SITE command to be executed before a file is downloaded. To find out what SITE commands are supported by the current FTP server, enter this command at the FTP command line: `QUOTE help site` This feature is not available for SFTP connections.

Upload to server options

Remove file name extension	Remove the filename extension from files transferred to the host. If an uploaded file's name contains one or more dots, the final dot and any subsequent characters are removed from the filename.
Prepend these characters to the file name	Add the specified characters before the filename for files copied to the host. For example, you can use this feature to specify a member name for transfers to an IBM host. If you are connected to an HP POSIX host, the client automatically sets this value to a period followed by a slash (./).
Server file name limit	Set a limit to the number of characters in the filename for files transferred to the host. Filenames beyond this limit are truncated.
Set case of long file names	Select how case is handled in when the transferred filename does not conform to the DOS 8.3 file naming convention.
Set case of 8.3 file names	Select how case is handled when the transferred filename does conform to the DOS 8.3 file naming convention.
Compute space on MVS	By default, the FTP Client computes and preallocates the number of tracks on MVS system based on the local file size. Clear this option to disable this feature. This setting applies to uploads to MVS hosts only.
Send SITE command before transfer	Type a SITE command to be executed before a file is uploaded. To find out what SITE commands are supported by the current FTP server, enter this command at the FTP command line: `QUOTE help site` This feature is not available for SFTP connections.
Show upload options before transfer	Select this option if you want to be queried for the transfer method (for example, ASCII or binary) and file permission attributes before uploading a new file to the server.

Related Topics

- "Handle Existing Files (Transfer Mode)" on page 807
- "Resume an Incomplete Server File Download" on page 810
- "Directories Tab (Site Properties Dialog Box)" on page 798
- "Set Time and Date of Downloaded Files" on page 808

Information Tab (Site Properties Dialog Box)

Getting there

1 Start the FTP Client.

   This opens the **Connect to FTP Site** dialog box. (If the FTP Client is already running and this dialog box is not open, go to **Connection** > **Connect**.)

2 From the **Connect to FTP Site** dialog box, select a site.

3 Click the **Properties** button.

NOTE

- If you are already connected to a site, from the **Connection** menu, choose **Site Properties**.

- Some changes you make using the **Site > Properties** dialog box when connected will not take effect until the next time you connect to the site.

This tab shows information about the current FTP Client connection. It is available only when you are connected to a site.

Click **Reset** to reset the transfer time and transfer rate data to zero

Transferring Files

In this Section

Transfer Files with FTP Client

You can transfer files in the FTP Client with a simple drag and drop operation. You can drag individual files, multiple files, and entire folders.

To transfer files with FTP Client

1 Connect to an FTP site.

2 Specify a transfer method (**Tools** > **Transfer Method**).

3 Set the preference for handling existing files. (**Tools** > **If File Exists**).

   NOTE: Additional file transfer settings are available from the *Site* > **Properties** dialog box. You can use these site-specific properties to configure file transfer.

4 Browse to locate the files or folders you want to transfer and the destination location.

5 Select the files or folders you want to transfer and drag them from the source location to your desired destination.

NOTE: If you prefer to transfer files using FTP (or SFTP) file transfer commands, you can initiate transfers directly from the FTP command line.

Related Topics

- "Connect to a Site" on page 775
- "Set the Transfer File Type (Transfer Method)" on page 805
- "Handle Existing Files (Transfer Mode)" on page 807
- "View the Local PC Files" on page 772
- "View the Server Files" on page 773
- "Use the FTP Command Line" on page 839

Set the Transfer File Type (Transfer Method)

Use **Transfer Method** to specify the file type for transfers. The currently active transfer method is indicated on the status bar, on the toolbar, and in the **Transfer Method** menu.

To change the current file transfer method

- From the **Tools** menu, point to **Transfer Method** and then click the transfer method you want to use.

The options are:

ASCII

Select **ASCII** for text files. ASCII data is transferred according to settings in the **Character Sets** dialog box.

Binary

Use the **Binary** transfer method to transfer binary files, such as `.exe` files and `.doc` files. Binary files are not converted or translated during the transfer.

Tenex (Local 8)

Select **Tenex** (also known as "Local 8") if you're moving files to or from a server that uses a non-8-bit byte, such as the DECsystem-20.

Smart

Select **Smart** if you want the FTP Client to determine what transfer method to use (**ASCII, Binary, Tenex,** or **Ask User)** based on the source file extension. To configure this, use **Tools** > **Options** > **File Types**.

Related Topics

- "Character Sets Dialog Box" on page 812
- "Add a Smart File Transfer Type" on page 806

Add a Smart File Transfer Type

Use the Smart transfer method if you want the FTP Client to determine which transfer method to use (**ASCII, > Binary**, **Tenex**, or **Ask User)** based on the source file extension. When performing a Smart file transfer, the client refers to the list of Smart file types to determine what transfer method to use for the current file. You can add file types to the default Smart file types list, or change the file transfer method used for existing file types. For example, you might specify that files with names ending in `.doc` use the **Binary** transfer method.

To add a new Smart file transfer type

1   From the **Tools** menu, choose **Options**.

2   Click the **File Types** tab.

3   Click **New**.

4   Use the following settings from the **Add Smart File Type** dialog box to define a new file type:

For this setting	Do this
File type	Type the file type extension that identifies this file type, or select a file type from the list.
Transfer method	Select a transfer method for files of this type.
	This setting determines how files of this type are saved, and any data manipulation that should be performed during the transfer.

NOTE

- To define a transfer method for files that don't have an extension, choose **<none>** in the **File type** box, and then select a transfer method.
- If a file extension might identify files of several types, you can specify **Ask User** as the transfer method for that extension.

Related Topics

Specify a Default Smart File Transfer Type

The default Smart transfer type applies to any file types that have not been defined previously.

To specify a default Smart file transfer type

1   From the **Tools** menu, choose **Options**.

2 Click the **File Types** tab.

3 Under **Transfer method for undefined file types**, select a transfer type.

NOTE: If you have files that have the same file extension, but require a different transfer method, do not set a default type. Set **Transfer method for undefined file types** to **Ask User**. Or, set the file transfer method you want to use prior to transferring the file(s).

Related Topics

- "Set the Transfer File Type (Transfer Method)" on page 805
- "Add a Smart File Transfer Type" on page 806

Handle Existing Files (Transfer Mode)

You can set a transfer mode to specify how the FTP Client should handle transfer when a file with the same name already exists in the target location. The current transfer mode is indicated on the status bar next to the transfer method.

To specify how to handle existing files

- From the **Tools** menu, point to **If File Exists** and then click the transfer mode you want to use.

Append	Append the downloaded file to the destination file. This option is only available for transfers from the host.
Ask User	Open the **Confirm File Replace** dialog box to allow the user to decide what to do.
Cancel	The file transfer is canceled when a file with the specified name already exists.
	If the file is part of a wildcard set (files being transferred using wildcards or a string of filenames), no other files are transferred to the PC after a duplicate is found.
Overwrite	Overwrite the destination file.
Skip	Do not transfer this file. If additional files are specified for this transfer operation, continue with the next file.
Update	Overwrite the destination file only if the file being transferred is newer than the destination file.
Unique	Automatically create a unique name for the destination file. The names of any files that are renamed during the transfer operation are shown in the FTP command window.

NOTE: In some circumstances, this setting is ignored. The value you specify using the **If File Exists** command applies only to transfers within the FTP Client. If you use drag-and-drop to transfer a file from a client display pane to your desktop or an open Windows Explorer window, Windows will always display a **Confirm File Replace** dialog box whenever a file exists, regardless of the FTP Client configuration. To take advantage of the currently configured option, always use Reflection panes for drag-and-drop transfers.

Related Topics

Set Time and Date of Downloaded Files

1 Open the **Site Properties** dialog box and then click the **Transfer** tab.

2 Select **Preserve server file date** if you want all files transferred from the server to retain the original time and date. Clear this box if you want files transferred from the server to be stamped with the time and date when they were transferred.

Related Topics

Transfer Files between Two Remote Sites

You can use the FTP Client to drag files between two remote sites.

To transfer files between two remote sites

1 Connect to your first server site.

2 From the **Connection** menu, click **Connect to a second site**.

The server pane will display files and folders for both sites.

3 Use the drag-and-drop method to transfer files directly from one server to another.

NOTE

- If the transfer type is **Binary** and both connections are configured without security features in place (such as use of a proxy server, Secure Shell, port forwarding, or sftp) the data is transferred directly over the data channel between the two sites.

- If there is a secure connection to either server, or the transfer type is not **Binary**, the client downloads the file to a temporary location on your PC and then uploads it to the other site. The temporary file is deleted after the transfer is complete.

Related Topics

Change the Filename when Downloading

The **Download As** command is available when you right-click on a file in the server pane. You may prefer this command over drag-and-drop file transfer when you want to transfer a server file to your PC and use a different file name on the PC.

To download a file using a different name

1 Right-click on the file you want to download, and then choose **Download As**.

2 From the **Download As** dialog box, in the **Download As** box, type the name you want to use for the file on the PC.

3 Click **OK** to complete the transfer.

Also, wildcard characters are supported. You can download multiple files at once, changing all of the filenames. For example, you could change all of the `.htm` files in a directory to `.html` when you download them to your PC.

To download multiple files using a different name

1 Right-click on one of the files you want to download, and then choose **Download As**.

2 From the **Download As** dialog box, in the **Server file(s)** box, replace one or more parts of the filename with wildcards, leaving enough to identify which files you want.

   For example, `*.htm`. or `*_info_??.text`

3 From the **Download As** dialog box, in the **Download As** box, make the same wildcard replacements, and change the part of the filename you want to make different on your PC.

   For example, `*.html`. or `*_info_??.txt`.

4 Click **OK** to complete the transfer.

Related Topics

◆ "View the Server Files" on page 773

◆ "Transfer Files with FTP Client" on page 804

Change the Filename when Uploading

The **Upload to Server** command is available when you right-click on a file in the left pane of the FTP Client. You may prefer this command over drag-and-drop file transfer when you want to transfer a local file to the server and use a different file name on the server.

To upload a file using a different name

1 Right-click on the file you want to upload, and then choose **Upload As**.

2 From the **Upload As** dialog box, in the **Upload As** box, type the name you want to use for the file on the server.

3 If you are connected to two remote sites, both site names will appear in the **Upload As** dialog box. Select the site to which you want the file transferred.

4 Click **OK** to complete the transfer.

Also, wildcard characters are supported. You can upload multiple files at once, changing all of the filenames. For example, you could change all of the `.htm` files in a directory to `.html` when you upload them to the server.

To upload multiple files using a different name

1 Right-click on one of the files you want to upload, and then choose **Upload As**.

2 From the **Upload As** dialog box, in the **Source file(s)** box, replace one or more parts of the filename with wildcards, leaving enough to identify which files you want.

   For example, `*.htm`. or `*_info_??.text`

3 From the **Upload As** dialog box, in the **Upload As** box, make the same wildcard replacements, and change the part of the filename you want to make different on your server.

   For example, `*.html`. or `*_info_??.txt`.

4 Click **OK** to complete the transfer.

Related Topics

Resume an Incomplete Server File Download

Sometimes when downloading a server file to your PC, the transfer does not complete successfully, perhaps due to a loss of the network connection on a "noisy" or low-speed link.

NOTE: This feature is not available for SFTP connections.

When a file transfer fails to complete, the auto resume feature lets you resume the incomplete file transfer operation. The auto resume feature works only under these circumstances:

* The FTP server must support the REST command

   To auto resume a file transfer, the FTP Client sends a REST command (restart) to the server. If the server does not support the REST command, the file transfer will start from the beginning of the file. For each site, after the first auto resume operation is attempted, the FTP Client will remember the result. If the server does not support the REST command, the Client won't attempt to perform an auto resume for any file transferred from that server.

   To determine if a particular server supports this feature, enter the following on the command line:

   ```
   quote help rest
   ```

   If `rest` is identified as a restart command, your server supports the feature

* File transfer method (or type) must be Binary

   Auto resume compares the size of the source file to the size of the incomplete target file to determine at what point in the source file it should resume the transfer. An ASCII file transfer creates a file on the local machine that may differ in size from the source file.

- File transfer mode cannot be Append

  When you transfer a file using the Append mode, the FTP Client can't use the existing target file size to determine the restarting point to use in the source file.

To resume an incomplete download

1 If necessary, reconnect to the server where the source file resides.

2 Confirm the three circumstances above.

3 From the **Transfer** tab of the **Site Properties** dialog box, select **Try to resume partial binary downloads**.

4 Restart the server file download. For example, select the server file that failed to transfer and drag it again to the destination on your PC.

5 The client detects that a prior incomplete file transfer operation occurred for that file, and gives you the option to resume the incomplete transmission at the interruption point, instead of beginning a new file transfer of the entire file.

6 Click **Resume**.

Related Topics

- "Set the Transfer File Type (Transfer Method)" on page 805
- "Handle Existing Files (Transfer Mode)" on page 807
- "Transfer Tab (Site Properties Dialog Box)" on page 801

Character Sets Dialog Box

Getting There

1 From the **Connect to FTP Site** dialog box, select a site, and then click the **Properties** button.

   -Or-

   If you are already connected to a site, from the **Connection** menu, choose **Site Properties**.

2 Click the **Translation** tab. and then click the **Character Sets** button.

The need to translate characters is dictated by differences between the character set used by the source and the character set used at the destination. In most situations, no translation is necessary.

- If both client and server use the DOS character set, no translation is necessary.
- If the client uses the Windows character set and the server uses the ISO-Latin-1 character set, no translation is necessary.

The FTP Client can translate between the server character set and either the Windows or DOS character set. These settings apply to ASCII file transfers and characters sent from the server that are written to the screen.

NOTE: This feature is not available for SFTP connections.

The options are:

Translate files	Enable translation of ASCII files. Character translations occur when a PC file is sent to the server and when characters sent from the server are written to a client file.
Translate server messages	Enable translation when characters sent from the server are written to the screen.
Detect server Kanji type	Specify that character translation should be based on the type of Kanji character set detected in a file or message. This option is available only when **Server** is set to **EUC**, **DEC 1983 Kanji**, or **JIS X0208-1983**, and either **Translate files** or **Translate server messages** is selected.
	Clear this check box to use the specified **Server** Kanji character set at all times.
Client	Specify the character set to use on the client PC when **Translate files** is selected.The default setting is the current Windows character set.
Server	Specify the character set to use during ASCII file transfers (if **Translate files** is selected) and when translating server messages (if **Translate server messages** is selected).
ISO-7/NRC	Specify the national character set (NRC) to use for replacement purposes. Translation replaces certain characters from the ASCII set with accented characters and symbols for a specific national language.
	This option is only available when the **Server** character set is **DEC Supplemental, ISO Latin-1**, or **HP Roman 8** and **Change Roman-8 to ISO-7** and **Change ISO-7 to Roman-8** are selected, or **Change MCS to NRC** and **Change NRC to MCS** are selected.

To server

These options are available only when either **Translate files** or **Translate server messages** is selected.

Change Roman-8 to ISO-7	If **ISO-7/NRC** is set to a value other than **US ASCII**, select this option to have Roman 8 characters translated to an equivalent ISO-7 character when possible. The **ISO-7/NRC** value determines the character conversion.
	This option is available only when the **Server** character set is **HP Roman 8**.
Change MCS to NRC	Specify whether characters are translated from the DEC multinational character set (MCS) to the current national replacement character (NRC) set. The **ISO-7/NRC** value determines the character conversion.
	This option is available only when the **Server** character set is **DEC Supplemental** or **ISO Latin-1**.

Half- to full-width Katakana	Specify whether characters are translated from the current half-width Katakana character set to the full-width Katakana character set.
	The **Server** value determines which Kanji character set is used during the conversion.
	This option is available only when the **Server** character set is one of the JIS types (except Shift-JIS), the two DEC Kanji types, and EUC (Unicode).

From server

These options are available only when either **Translate files** or **Translate server messages** is selected.

Change ISO-7 to Roman-8	If **ISO-7/NRC** is set to a value other than **US ASCII**, select this option to have ISO-7 characters converted to equivalent Roman 8 characters. The **ISO-7/NRC** value determines the character conversion.
	This option is available only when the **Server** character set is **HP Roman 8**.
Change NRC to MCS	Specify whether characters should be translated from the current national replacement character (NRC) set to the DEC multinational character (MCS) set. The **ISO-7/NRC** value determines the character conversion.
	This option is available only when the **Server** character set is **DEC Supplemental** or **ISO Latin-1**.
Full- to half-width Katakana	Specify whether characters are translated from the current full-width Katakana character set to the half-width Katakana character set.
	The **Server** value determines which Kanji character set is used during the conversion.
	This option is available only when the **Server** character set is one of the JIS types (except Shift-JIS), the two DEC Kanji types, and EUC (Unicode).

Related Topics

Add Smart File Type Dialog Box

Getting There

1 From the **Tools** menu, choose **Options**.

2 Click the **File Types** tab, and then click **New**.

When Smart file transfer is enabled, all filenames with a specified extension are transferred using the associated transfer method.

File type	Type a file extension to associate with a specific transfer method, or select a file type from the list.
Transfer method	Select the transfer method you want to use for files with this extension.

Related Topics

- "Set the Transfer File Type (Transfer Method)" on page 805
- "Add a Smart File Transfer Type" on page 806
- "Specify a Default Smart File Transfer Type" on page 807

Smart Transfer File Type Dialog Box

This dialog box appears when you have selected the **Smart** transfer method and you are transferring a file with an undefined file type. Specify what transfer method you want to use for files with this file extension.

NOTE: Save your settings file to add this association permanently to your **Smart** file transfer list.

The options are:

ASCII	Use ASCII transfer for text files, such as `.txt` and `.html`.
Binary	Use binary transfer for binary files, such as `.exe` files and `.doc` files. Binary files are not converted or translated during the transfer.
Tenex	Use Tenex (also known as "Local 8") if you're moving files to or from a server that uses a non-8-bit byte, such as the DECsystem-20.
Always ask user	Select this option if you always want to be asked how to handle files with this extension. For example, you might want to select this option if the same file extension is used for different file types.
	NOTE: This option is not available if **Always ask user** has already been specified for this file type.

Related Topics

- "Add a Smart File Transfer Type" on page 806
- "Set the Transfer File Type (Transfer Method)" on page 805

Confirm File Replace Dialog Box

When **If File Exists** is set to **Ask User**, this dialog box opens each time a client or server file being transferred already exists on the destination. The options are:

Append server file to local file	Append the downloaded file to the destination file. This option is only available for transfers from the host.
Overwrite local/server file	Overwrite the destination file.
Skip this file	Do not transfer this file. If additional files are specified for this transfer operation, continue with the next file.
Copy to a different name	Type in the new filename to use in the destination folder, and click **OK.**
Copy using a unique name	Automatically create a unique name for the destination file. The names of any files that are renamed during the transfer operation are shown in the FTP command window.
Update local/server file if older	Overwrite the destination file only if the file being transferred is newer than the destination file.

Related Topics

Managing Files and Folders

In this Section

Working with Files

Commands on the **File** and **Edit** menus, and most buttons on the toolbar, apply to folders and files in the currently active pane. These commands let you rename, delete, and do other directory management tasks within the FTP Client.

Also, you can right-click a file to access commands in the context menu. For example, to get information about a file, right-click it and choose **Properties**.

Double-click a file to open or run it.

NOTE: In order to display the contents of a server file or run a program located on the server, the file is copied from the server to your Windows user folder.

Related Topics

- "Working with Local Folders" on page 816
- "Working with Server Directories" on page 817
- "Working with Filename Characters" on page 819
- "Filter the Server File Listing" on page 820

Working with Local Folders

To work with items on the local PC, use the left pane of the FTP Client. You can browse disk drives on your computer or local network, create new folders, and do other directory management tasks within the FTP Client. Commands on the **File** and **Edit** menus, and most buttons on the toolbar, apply to folders and files in the currently active pane.

New folders can be added from the **File** menu, context menu (right-click), or toolbar. Use the context menu to create shortcuts to folders.

To view the local directory structure, use the **Go to a different folder** list box in the upper left corner of the main window. To see how the current folder fits in the hierarchy on your computer, click the down arrow in the list box. The **Tools** menu and toolbar provide access to the **Up One Level** command. Also, you can navigate directly to a folder using the **Go to** command.

To navigate directly to a local folder

1 From the **Tools** menu, choose **Go to**.

2 Type the name of the directory you want to open.

   For example: `J:\Payroll\July`.

3 Select **Local Computer** to indicate that the folder is available on your PC.

NOTE: You can enter UNC (Universal Naming Convention) names for directory paths. There is a 47-character limit for UNC names, and each name can contain any character, both uppercase or lowercase, except the following: `?  "  /  |  <  >  *  :`

The syntax of a UNC name is as follows:

`\\<computername>\<sharename>\<pathname>`

Related Topics

- "View the Local PC Files" on page 772
- "Set Default Home Directories" on page 818
- "Create a Shortcut to a Local File or Folder" on page 817

Create a Shortcut to a Local File or Folder

To create a shortcut to a local file using the FTP Client

1 In the left pane, select the files and folders you want to create shortcuts to.

2 Click the right mouse button to open the context menu.

3 From the context menu, click **Create Shortcut** to create a shortcut to each of the selected files and folders.

   The shortcuts are created in the current folder on the PC.

Related Topics

- "Working with Local Folders" on page 816
- "Working with Files" on page 816
- "View the Local PC Files" on page 772

Working with Server Directories

To work with items on the server, use the right pane of the FTP Client. You can browse remote directories, create new folders, and filter the file listing. Commands on the **File** and **Edit** menus, and most buttons on the toolbar, apply to folders and files in the currently active pane.

New folders can be added from the **File** menu, context menu (right-click), or toolbar.

To view the remote directory structure, use the **Go to a different folder** list box in the upper left corner of the main window. To see how the current directory fits in the hierarchy on your server site, click the down arrow in the list box. The **Tools** menu and toolbar provide access to the **Up One Level** command. Also, you can navigate directly to a remote directory using the **Go to** command.

To navigate directly to a remote directory

1 From the **Tools** menu, choose **Go to**.

2 Type the name of the directory you want to open.

   Follow the server's syntax for directory names.

3 Select *site name* to indicate that the directory is located on the server.

Related Topics

- "View the Server Files" on page 773
- "Set Default Home Directories" on page 818
- "Filter the Server File Listing" on page 820
- "Run the Directory Definition Wizard" on page 821

Set Default Home Directories

Use default home directories to determine which files you see by default in the FTP Client. The default server directory determines which files you see in the server pane when you first connect to a site. There are two kinds of default local home folders. One is the global setting for the FTP Client,

and the other kind is specific to each site that you connect to. Once you've configured a site-specific local home folder, the FTP Client will show that folder in the local pane, and the default server home directory in the server pane.

To set the default server directory

1 Use the right pane to browse for the server directory you want to set as the default.

2 From the **Connection** menu, choose **Site Properties** and then click the **Directories** tab.

3 Under **Server**, click **Use Current**.

   This enters the current server location in the **Home directory** text box.

4 Click **OK**.

NOTE: To change the default server home directory, you can also right-click the folder you want to use, and then choose **Set Home Directory**.

To set the default local folder for a specific site

1 From the **Connect to FTP Site** dialog box, select a site, and then click the **Properties** button.

   -Or-

   If you are already connected to a site, from the **Connection** menu, choose **Site Properties**.

2 Click the **Directories** tab.

3 Under **Local**, click **Browse** and select the PC directory you want to set as the default.

4 Click **OK**.

To set the default local folder for the FTP Client

1 From the **Tools** menu, choose **Options**.

2 Click the **Directories** tab.

3 Under **Default local home folder**, click **Browse** and select the PC directory you want to set as the default.

4 Click **OK**.

Related Topics

- "Directories Tab (Site Properties Dialog Box)" on page 798
- "General Tab (Options Dialog Box)" on page 792
- "Working with Local Folders" on page 816
- "Working with Server Directories" on page 817

Working with Filename Characters

The FTP Client supports long filenames. Long filenames in Windows can contain spaces. The only characters that are not allowed are:

\ / : * ? " < > |

The following length limitations apply:

- Maximum path (excluding the filename): 246 characters (including drive letter, `:` character and `\` character). This limit of 246 allows for the addition of a filename in the standard 8.3 format with the terminating null character.

- Maximum filename: 256 characters (including terminating null character)

- Maximum fully qualified name (path + filename): Varies slightly with different Windows operating systems. Use 259 characters to ensure a valid path for all Windows systems.

Working with filenames that contain spaces

When you use FTP or SFTP commands, any filename that contains spaces must be enclosed in double quotation marks. For rules on how quotation marks are used, see the "Quotation Marks in FTP or SFTP Commands" on page 841 topic.

Working with server filenames that contain prohibited characters or are too long

For file transfers to the PC, the FTP Client automatically ensures that the name given to the file on your PC is valid in Windows by using the following rules:

- Strip all illegal characters. Example: `fast*lane` becomes `fastlane`.

- Invalid characters are: `\  /  :  *  ?  "  <  >  |`

- If necessary, truncate the filename. In Windows, the length limitations described above are applied.

- The Windows path is always preserved. If the server filename plus the destination Windows path is greater than the maximum allowed, the server filename is truncated.

- If the filename begins with a period, the appropriate number of characters are removed from the end of the filename. If the filename contains periods, the client determines the location of the last period in the name and truncates the appropriate number of characters to the left of the period.

If you want transfers from a server site to automatically derive a valid DOS name when the server filename is too long or when it contains invalid characters, select the **Create Windows file names in 8.3 format** option on the **Transfer** tab in the **Site Properties** dialog box.

Related Topics

- "Quotation Marks in FTP or SFTP Commands" on page 841
- "Working with Files" on page 816
- "Transfer Tab (Site Properties Dialog Box)" on page 801

Filter the Server File Listing

Using a file filter allows you to view a subset of the files on the server. You can specify a default file filter or a temporary file filter. If the server directories contain a lot of files, specifying a default filter provides a way to speed up retrieval and display of directory listings.

NOTE: This feature is not available for SFTP connections.

To specify a default file filter for a server

1 From the **Connection** menu, choose **Site Properties** and then click the **Directories** tab.

2 In the **File View Filter** box, type a default view filter for all server directory listings for that site.

For example, type `*.txt`to list all files in the current directory that end in `.txt`. The specification must use wildcard characters that are recognized by the type of server running at the site.

3 Click OK.

The FTP Client automatically refreshes the server directory listing.

To apply a temporary file filter

1 From the **View** menu, choose **Filter**.

2 In the **Server View Filter** dialog box, type a view filter specification.

For example, type `*.txt`to list all files in the current directory that end in `.txt`. The specification must use wildcard characters that are recognized by the type of server running at the site.

3 Click OK.

The FTP Client automatically refreshes the server directory listing.

NOTE

- If you are connected to two servers in the same session, the **View** menu **Filter** command applies to both servers. To apply a filter to only one server, right-click in the display pane for that server, and select **Filter** from the context menu.

- When a view filter is in effect, the filter is shown in the title bar of the server pane.

- To request a listing of all files in the folder, type * (asterisk) for your view filter specification.

Related Topics

- "Working with Server Directories" on page 817
- "Server View Filter Dialog Box" on page 823
- "Directories Tab (Site Properties Dialog Box)" on page 798

Run the Directory Definition Wizard

The **Directory Definition Wizard** helps you to define the directory format for an unrecognized type of FTP server. The Wizard allows you to identify the filename and other fields in the directory output from the current FTP site so that server directory listings can be displayed and interpreted properly in the right pane of the FTP Client window.

NOTE: This wizard should not be used if the files on the FTP site already display properly.

To use the Directory Definition Wizard

NOTE: To use the Directory Definition Wizard, you must have **Server type** set to **Auto detect** (the default value) on the **General** tab of the Site Properties dialog box.

---

1 Connect to a site.

2 From the **Tools** menu, choose **Directory Definition Wizard**.

3 Complete the steps as directed by the wizard.

NOTE: File name is the only required field. You can leave the other fields undefined.

---

4 When you are done specifying the location of fields, click **Finish**.

The FTP Client automatically refreshes the server directory listing.

5 If the directory listing is still unusable, re-run the **Directory Definition Wizard** and continue experimenting with the location of directory fields until you get better results.

Related Topics

- "FTP Client Troubleshooting" on page 828

Set File and Directory Permissions

You can change file permissions on the server using the server pane or the FTP command line. You can also configure global defaults for new files and directories. For individual sites, you can configure the client to query you for permission values each time you transfer a file or create a new directory.

To change file and directory permissions using the server pane

1 Connect to a UNIX or Linux host.

2 In the server pane, select one or more files or directories.

3 Right-click your selection and choose **Properties**.

4 Change the attributes of the selected item(s) using either of the following techniques:

- In the **Permission Mode** box, type a three digit number that is a valid value for the UNIX **chmod** command. Valid values have digits from 0 to 7.
- Under **Owner**, **Group**, and **Public**, select options to allow each user type permission to read, write, or execute.

5 Click **OK**.

To configure global defaults for transferred files or newly created directories

1 Go to **Tools** > **Options**

2 To set default permissions for uploaded and downloaded files, use the **File Attributes** tab.

3 To set default permissions for newly created directories, use the **Directory Attributes** tab.

4 Click **OK**.

To set permissions each time you transfer a file or create a directory

1 Open the site properties dialog box.

 ◆ To set permissions each time you create a directory on the server, click the **Directories** tab and select **Show attributes before creating directory**.

 ◆ To set permissions each time you transfer a file, click the **Transfer** tab and select either or both of the following options: **Show download options before transfer** and **Show upload options before transfer**.

2 Click **OK**.

To change file and directory permissions using the FTP command line:

1 Connect to a UNIX or Linux host.

2 Press F7 to display the command line if it is not already visible.

3 Enter a UNIX **chmod** command using a numeric permission mask.

 For example, the following commands sets attributes to `-rw-r--r--` for the specified file.

 ```
 chmod 644 myfile.htm
 ```

NOTE: Permissions changes you make to directories are not recursive; that is they do not affect the files within the directory.

Related Topics

 ◆ "Use the FTP Command Line" on page 839
 ◆ "Server File Properties Dialog Box" on page 823
 ◆ "Set Time and Date of Downloaded Files" on page 808
 ◆ "Change the Filename when Downloading" on page 809
 ◆ "Change the Filename when Uploading" on page 810

Server View Filter Dialog Box

Getting there

 ◆ From the FTP Client **View** menu, choose **Filter**.

Use the **Server View Filter** dialog box to request a remote site directory listing that shows server files of a specific type.

Type a wildcard specification. For example, type `*.txt` to list all files in the current directory that end in `.txt`. The specification must use wildcard characters that are recognized by the type of server running at the site. When you click **OK**, the server directory listing refreshes in the right pane, showing only the files that match your specification.

NOTE

 ◆ This feature is not available for SFTP connections.

- When a view filter is in effect, the filter is shown in the title bar of the server pane.
- To request a listing of all files in the folder, type * (asterisk) for your view filter specification.

Server File Properties Dialog Box

Getting there

1 Start the FTP Client.

   This opens the **Connect to FTP Site** dialog box. (If the FTP Client is already running and this dialog box is not open, go to **Connection** > **Connect**.)

2 Connect to a site and then select a file or folder in the server pane.

3 From the **File** menu, choose **Properties**.

This dialog box displays information about the currently selected server file or directory. You can also use it to set permissions on a UNIX or Linux server.

Permissions changes you make to directories are not recursive; that is they do not affect the files within the directory.

Attributes	Displays the current attributes.
Permission Mode	Type a three digit number that is a valid value for the UNIX **chmod** command. Valid values have digits from 0 to 7.
Owner, Group, and Public	Select options to allow each user type permission to read, write, or execute the currently selected item.

Related Topics

- "Set File and Directory Permissions" on page 821
- "Working with Server Directories" on page 817

Go To Folder Dialog Box

Getting there

- From the FTP Client **Tools** menu, choose **Go to**.

Type the name and path of the folder you want to open.

- Click **Local Computer** to specify a path on the local computer.
- If you are connected to a server, the server name is shown. Click this option to specify a path on the server.

Related Topics

- "Working with Local Folders" on page 816
- "Working with Server Directories" on page 817

Customizing FTP Client Startup

You can customize how the FTP Client starts using shortcuts, startup switches, and script files. You can use Windows shortcuts to provide quick and easy access to the Reflection FTP Client and to your servers. You can create a shortcut to:

- ◆ Open a settings file and display a list available sites
- ◆ Connect to a specific host site

In this Section

Create a Shortcut to Load a Settings File

You can create a shortcut that loads an FTP Client settings file and automatically opens the **Connect to FTP Site** dialog box showing a list of available sites.

To create a shortcut that launches the FTP Client and loads a settings file

1 From the **File** menu, select **Save As**.

2 (Optional) Type a new name for the file you are saving.

3 Select the **Save shortcut on desktop** option in the lower left corner of the **Save Settings** dialog box.

4 Click **Save**.

Related Topics

Create a Shortcut to Connect to a Site

You can create a shortcut that launches the FTP Client and automatically connects to a server.

To create a shortcut that launches the FTP Client and connects to a site

1 The **Connect to FTP Site** dialog box opens when you start the FTP Client. You can also open it by choosing **Connect** from the **Connection** menu.

2 Right-click on any site in the list and select **Create Shortcut**.

You will see a message telling you that a shortcut has been created on the desktop.

3 Click OK.

Related Topics

◆ "Connect to FTP Site Dialog Box" on page 772

FTP Client Startup Switches

You can start the FTP Client and provide command line parameters that automatically connect to a predefined site, run a specified script file, connect using a settings file, or connect to a server specified with a URL.

◆ You can set up a shortcut with a startup command that automatically executes the startup command when you double-click it. The properties you specify for the shortcut determine whether the Client runs in a window or runs minimized on the desktop when you start it.

◆ You can enter a startup command in the **Open** box when you use the **Run** command on the **Start** menu.

Startup Command Syntax

```
<executable>.exe [<site>] /<switch> <parameter>
```

`<executable>.exe`	Provides the path and name of the FTP executable file, for example:
	`"C:\Program Files\Micro Focus\Reflection\rftpc.exe"`
`<site>`	Specifies a site defined in a settings file. The site properties are in effect when the client starts. If the site name contains spaces, enclose it in quotation marks, for example `"ADA Home"`.
	When included, the `<site>` argument is always the first argument on the command line. When used in conjunction with the `/W`switch, the `<site>` argument is ignored.
	If the defined site is not in the default settings file (Settings), use the `/RFW`switch to specify the settings file that includes the site definition.
`/<switch>` `<parameter>`	Use one or more of the switches listed below to specify the operations you want to perform when the client starts up:

Startup Switches

`/D <diagnostic file>`	Directs the client to record in the specified file all communications between the client and the server, as well as other diagnostic information that may be useful for troubleshooting. The specified diagnostic file is placed in your My Documents folder. This file is refreshed each time you start the client.
`/E`	Directs the client to log events to the Application event log. Note: The diagnostic file created with /D includes more detailed information than this event log.
`/FMIGRATE`	Launches the Reflection F-Secure Migration Wizard, which you can use to migrate F-Secure profiles to Reflection settings files.

`/L <log file>`	Directs the client to record in the specified log file all communication between the client and the server to which it connects. This is a cumulative log file; new information is added after existing information.
`/N`	Suppresses the display of the Reflection startup screen.
`/RFS <script file>`	Runs the specified script. If the script ends in a QUIT command, the client shuts down when the script completes.
`/RFW <settings file>`	Allows you to connect using the specified settings file.
`/X <export file>`	Launches the Export Settings dialog box directly without launching the main client window.

`/W <URL>`	Connects to the server specified in the <URL> parameter. The syntax is shown here:
	
	`rftpc[.exe] /W ftp://`
	`[username[:password]@]hostname[:port][/directory]`

`/?`	Displays the list of allowable start-up commands.

Related Topics

◆ "Startup Command Examples" on page 827

Startup Command Examples

The following example command runs the FTP Client (`Rftpc.exe`) and connects to a site named West Coast, which is defined in the default settings file.

`"C:\Program Files\Micro Focus\Reflection\rftpc.exe" "West Coast"`

In the example above, quotation marks must surround the executable file specification because the path specifies a folder name that contains a space. Similarly, the site name is surrounded by quotation marks because it contains a space in the name.

The next example command uses the `/W`switch to specify the URL for an FTP site and the `/L` switch to direct the FTP Client (`rftpc.exe`) to log all client/server communication to a log file named `Ftpinfo.log`.

`"C:\Program Files\Micro Focus\Reflection\rftpc.exe" /W ftp://ftp.myco.com /L Ftpinfo.log`

The following example command tells the FTP Client to connect using a settings file and run a script file. The `/RFW` switch directs the FTP Client to connect using the settings file `Myfile.rfw`. The `/RFS` switch directs the FTP Client to run the script file `Transfer.rfs` after connecting to the server specified in the settings file.

`"C:\Program Files\Micro Focus\Reflection\rftpc.exe" /RFW`
`"C:\Mypath\Myfile.rfw" /RFS "C:\Mypath\Transfer.rfs"`

Related Topics

◆ "FTP Client Startup Switches" on page 825

Run a Script File at Startup

You can start the client and provide command line parameters that automatically execute all the commands in a script file. This allows you to automate sequences of commands.

- You can set up a shortcut with a startup command that automatically executes a script when you double-click it. The properties you specify for the shortcut determine whether the client runs in a window or runs minimized on the desktop when you start it.
- You can enter a startup command in the **Open** box when you use the **Run** command from the **Start** menu.

Startup Command Syntax to Execute a Script File

`<executable>.exe [<site>] /RFS <script file>`

Use a space to separate each argument in the command line.

`<executable>.exe`

Provides the path and name of the FTP Client executable file.

For example:

`"C:\Program Files\Micro Focus\Reflection\Rftpc.exe" <site>`

Specifies a previously defined site. The site properties are in effect when the client starts. If the FTP site name contains spaces, enclose it in quotation marks, for example `"ADA Home"`.

When included, the `<site>` argument is always the first argument on the command line. When used in conjunction with the `/W`switch, the `<site>` argument is ignored.

`/RFS <script file>`

Provides the path and name of the FTP script file. If the script file name or path contains spaces, enclose it in quotation marks , for example `"C:\My Script Files\Get lab reports.rfs"`.

Related Topics

- "FTP Client Startup Switches" on page 825
- "Example of Starting the Client with a Script File" on page 828

Example of Starting the Client with a Script File

The following command runs the FTP Client, connects to the FTP site "Central" and executes an FTP script file named `Upload.rfs`.

`Rftpc.exe Central /RFS Upload.rfs`

In this example, the FTP Client starts and automatically connects to the FTP site "Central". The site properties defined for the "Central" FTP site are in effect when the script runs.

NOTE: Any site or script filename containing spaces must be enclosed in quotation marks. For example:

`Rftpc.exe "My Site" /RFS "Central files download.rfs"`

Related Topics

- "Run a Script File at Startup" on page 827
- "FTP Scripting" on page 841

FTP Client Troubleshooting

In this Section

- "Identifying the Source of the Problem" on page 829
- "Troubleshooting FTP Client Connections" on page 829
- "Troubleshooting FTP File Transfer Problems" on page 831
- "Troubleshooting FTP Directory Listing" on page 832
- "Secure Shell Log File" on page 832
- "Troubleshooting FTP Site-to-Site Transfer" on page 833
- "FTP Client Error messages" on page 834
- "Windows Sockets Error Messages" on page 835
- "Error Messages" on page 837

Identifying the Source of the Problem

When you encounter a problem with the Reflection FTP Client, it may help to compare the behavior to that of another client. You can use the Microsoft FTP client to open a connection to the FTP server where the problem occurs; then try using this client to duplicate the operation that causes the problem.

If you can duplicate the problem when you use a different FTP client, one of these conditions may apply:

- The server you are connecting to does not support the FTP operation you are attempting.
- The server you are connecting to is configured incorrectly.
- You are specifying incorrect information in your command (for example, you are specifying a non-existent path or filename when attempting a file transfer).

If the problem only occurs when using the Reflection FTP Client (you can't duplicate the problem when you connect to the server using a different FTP client), check the troubleshooting solutions.

Related Topics

- "Troubleshooting FTP Client Connections" on page 829
- "Troubleshooting FTP File Transfer Problems" on page 831
- "Troubleshooting FTP Directory Listing" on page 832
- "Troubleshooting FTP Site-to-Site Transfer" on page 833

Troubleshooting FTP Client Connections

Use this topic to troubleshoot problems making connections using the FTP Client.

Configuring Connections

- Did you enter your server name, user name, and password correctly? If you are connecting to a case-sensitive server, be sure to use the correct case when making these entries.

- Does your site use a passthrough server or SOCKS proxy server to ensure that only authorized users have access to server sites? If so, you should configure the client to connect via the firewall or SOCKS proxy server.

- When opening a connection, the server name you provide is resolved via the HOSTS file or a domain name server. If you have no domain name server on the local network and don't use a HOSTS file, you must specify the full IP address of the host server. For example: 124.24.36.85

- If the FTP server is not running on the remote system, you can't connect.

- Server response time can be affected by the distance between sites. If you see the message "Connection timed out" when trying to connect to a server, increase the value of **Timeouts in seconds** on the **Connection** tab of the **Site Properties** dialog box.

- If the FTP Client is unable to determine the server type, server directory listings may display incorrectly. You can use the **Directory Definition Wizard** to modify the directory format.

- If you are having trouble making a Secure Shell connection, use the Secure Shell log to get troubleshooting information.

Connection Troubleshooting

Error message: "Could not resolve host address."

Several things can cause this message to appear:

- The host name or IP address you entered for the server is invalid. Re-enter the host name; if you are connecting to a case-sensitive server, be sure to use the correct case.

- The host name you provide is resolved via the HOSTS file or a domain name server. Is the computer that acts as the domain name server working? Has the HOSTS file on your PC been corrupted? If no domain name server or HOSTS file is available, you must specify the full IP address of the host server. For example: 124.24.36.85.

- You have entered an IPv6 address, but have not enabled IPv6 support on your PC. Contact Microsoft for more information.

- You must have an appropriately configured IP router (gateway) in order to connect to servers outside your own network. Check to see whether the computer serving as the router is up and running.

Error message: "Connection timed out."

Server response time can be affected by the distance between sites. If you see this message when trying to connect to a server, increase the **Connect Timeout** setting to give the server more time to respond during the login process.

Reflection FTP hangs when you try to connect

On some systems, turning off the use of animation (such as showing a waving flashlight while you are waiting for a directory listing) fixes display problems that cause Reflection to hang when you attempt a connection. To disable the use of animation, open the **Tools** menu, click **Options**, open the **Preferences** tab and enable **Do not use animation**.

Host cannot respond to the PWD command

By default, Reflection sends a PWD command when you connect to your server. Some servers don't support this command. Press F7 to open the command window before you try connecting to your server. If the server returns an error after Reflection sends the PWD command, try enabling this setting. To configure Reflection to connect without the PWD command, open the **Directories** tab of the **Site Properties** dialog box and select **Don't send PWD Command**.

Error Message: PASV is not implemented by the server

By default, the client connects using the PASV command. This causes the client to initiate a separate data connection for directory listings and file transfers, which is required for connections through some firewalls. If your server does not support the PASV command, you can disable the **Use passive mode setting** on the **Connection** tab of the **Site Properties** dialog box.

Related Topics

- "Secure FTP Client Connections" on page 777
- "Connection Tab (Site Properties Dialog Box)" on page 796
- "Run the Directory Definition Wizard" on page 821
- "Secure Shell Log File" on page 832

Troubleshooting FTP File Transfer Problems

If you're having trouble transferring files using the FTP or SFTP client, consult the following list:

- You must be connected to a server before you can transfer files.
- If a transferred file is not usable (for example, you can't unzip a zipped file, you can't run an executable file, or you can't read an ASCII file), be sure that you are selecting the correct file transfer method prior to transferring the file.
- Transfers to a server may be unsuccessful if you don't have write permission to the destination directory on the server.
- If an "Access denied" message displays when you attempt to transfer a server file to your PC, you have a read-only file in the PC destination directory that has the same name as the file you are trying to receive, or you do not have write permission to the PC directory.
- If you see an error message when you attempt to transfer files between two remote hosts, the sending or receiving server may not be configured to support this feature.
- If a transferred ASCII file contains incorrect characters, you may need to use character translation to preserve the characters present in the source file when they are transferred to the destination file. When necessary, the FTP Client can translate between the server character set and either the Windows or DOS character set. Character translation ensures that characters present in the source character set are translated to characters available in the destination character set. For example, if you transfer files from a server that uses the DOS character set for

use in a Windows application, or if you want to transfer an ASCII file that contains accented characters and symbols for a specific national language, you need to set character translation options to perform necessary translation during file transfer. See the "Character Sets Dialog Box" on page 812 topic for more information.

 ◆ If you are having trouble transferring files when the file names contain spaces, quotation marks, or wildcard characters, see the "Quotation Marks in FTP or SFTP Commands" on page 841 topic for more information.

 ◆ If you are having trouble canceling a file transfer you may need to reconnect to the server. Some servers close your connection if you cancel a transfer while you are receiving (getting) a server file.

 ◆ If File Exists settings apply only to transfers within the Reflection FTP Client. If you use drag-and-drop to transfer a file from a FTP Client display pane to your desktop or an open Windows Explorer window, Windows will always display a Confirm File Replace dialog box whenever a file with the same name exists in the selected location, regardless of the configuration of the Reflection FTP Client. To take advantage of the currently configured FTP Client option, always use the FTP Client panes for drag-and-drop transfers.

Troubleshooting FTP Directory Listing

Consult the following list if you are having trouble obtaining directory listings at an FTP or SFTP site:

Trouble obtaining a directory listing or Server returns error "425 Can't open data connection"

If you don't see a directory listing in either the server pane or the command window, your server may not support the PASV command. Try clearing the Use passive mode setting in the Connection tab of the Site Properties dialog box.

Trouble seeing all files in a server directory

You may have specified a default wildcard filter for the site's server directory listings. The wildcard filter limits directory listings to files of a specific type. For example, if the filter specifies `*.txt`, directory listings will show only files that match the wildcard (that is, files ending in `.txt`).

 ◆ The default wildcard filter for server directory listings is set on the Directories tab in the Site Properties dialog box.

 ◆ When a wildcard filter is in effect, the filter will be shown in the title bar of the FTP Site pane (the right pane).

 ◆ To temporarily override the default wildcard filter for server directory listings, use View> Filter. To see all files and folders in the directory, type `*` (an asterisk).

Incorrect or empty server file display when connecting to a UNIX server using SFTP

Try changing the Use structured listing data setting (Site Properties > Security > Secure Shell) if you are connecting using SFTP and the server pane display is missing or is not correctly displayed. This setting specifies which data list style sent by the server is used to create the directory display in the right pane of the FTP Client. When this setting is not selected (the default), the FTP Client uses the standard UNIX-style data list. When it is selected, the FTP Client uses the structured data list.

You see an error message saying "The system cannot find the path specified" when you connect to the server

This error may indicate that the FTP Client is trying to find a local file path that does not exist. Check the local **Home** folder setting to be sure that the folder path exists on your computer. To view or edit this setting, open the **Site Properties** dialog box, click **Directories**, then find **Home folder** under **Local**.

Related Topics

 * "Run the Directory Definition Wizard" on page 821

Secure Shell Log File

Reflection maintains a log file with information about your last Secure Shell connection. Use either of the following techniques to view this log for the FTP Client:

 * Start logging (**Tools** > **Start Logging**) to send log information to a file.

 * Open the FTP command window (**View**> **Command Window**) to view the log on screen.

   NOTE: You can use the **Logging Level** setting to determine how much information is written to the Secure Shell log. This setting is available on the **Reflection Secure Shell Settings** dialog box -- General tab.

Troubleshooting FTP Site-to-Site Transfer

If you see any of the following error messages when you attempt to transfer files between two remote hosts, the sending or receiving server may not be configured to support this feature:

 * 500 Illegal PORT command

 * 501 IP address for data destination does not match client's

 * 425 Can't open data connection

 * 502 PASV command not implemented by this server

When the FTP Client encounters this problem, it attempts to transfer to the local PC, and then to the target site, after the error is received. Note that even though the transfer may complete successfully, you will see the error message before the transfer is completed.

If you regularly transfer between servers that don't support direct site-to-site transfer, you can configure the FTP Client to force all site-to-site transfers to copy files first to the local machine then to the destination server. This configuration allows you to transfer between sites without seeing one of the error messages listed above.

To force all site-to-site transfers to copy files first to the local computer

1 From the **Tools** menu, choose **Options**.

2 On the **Preferences** tab, select **Force site to site transfers through local machine**, and then click **OK**.

Review the following for more information about configuring servers to support direct site-to-site transfer.

Sending server configuration

Site-to-site transfer feature requires that any FTP server sending a binary file must accept a PORT command from the Reflection FTP Client to an IP address that is different from the client's IP address. (On some servers this support may be disabled for security reasons.) The PORT command specifies the TCP PORT to which the data should be sent. If the sending server does not accept this use of the PORT command, you will see two server error messages: usually a "500 Illegal PORT command" or a "501 IP address for data destination does not match client's" from the sending server, followed by a "425 Can't open data connection" from the receiving server. You will also see a file of zero bytes created on the receiving server because the file index is created prior to receiving any data. To enable site-to-site transfer, contact the administrator of the sending server to determine whether PORT commands to a different IP address can be enabled on the server.

Receiving server configuration

Site-to-site transfer requires that any FTP server receiving a binary file must accept a PASV command from the Reflection FTP Client and return the PORT information to be passed on to the sending server. If the receiving server does not accept the PASV command, the site-to-site transfer will fail with an error message: "502 PASV command not implemented by this server". To enable site-to-site transfer, contact the administrator of receiving server to determine whether PASV can be enabled on the server.

Related Topics

- "Transfer Files between Two Remote Sites" on page 808

FTP Client Error messages

Following is a list of the FTP Client error messages that may appear and an explanation of how to resolve the error condition.

A connection has not been established.

Command line error. You issued a command to a server (for example PWD, CD, DIR, LS, or QUOTE <command>) but you aren't currently logged in to the server. Open a server connection.

Access denied.

You cannot access the protected file or folder. Check that you have correct permissions for the operation you attempted.

Already connected to a site.

Command line error. You issued an OPEN or PASSTHRU command, but you are already logged in to a server. Use the CLOSE command to close the current connection prior to opening a new one.

Connection timed out.

When connecting to a server, the FTP Client waits up to <n> seconds for a response from the server. If nothing is received within the period specified, this message is displayed; in this case, try to connect again. If the message appears again, increase the connection timeout value to give the server more time to respond during the login process. To do this, open the **Connection** tab and edit the **Connect** text box under **Timeout in seconds**; or enter SET TIMEOUT-CONNECT at the command line.

Could not resolve host address.

Several things can cause this message to appear:

- The host name or IP address you entered for the server is invalid. Re-enter the host name; if you are connecting to a case-sensitive server, be sure to use the correct case.

- The host name you provide is resolved via the HOSTS file or a domain name server. Is the computer that acts as the domain name server working? Has the HOSTS file on your PC been corrupted? If no domain name server or HOSTS file is available, you must specify the full IP address of the server. For example: 124.24.36.85.

- You must have an appropriately configured IP router (gateway) in order to connect to FTP or SFTP servers outside your own network. Check to see whether the computer serving as the router is up and running.

Command <command>needs more arguments.

Command line error. The command you entered requires one or more arguments. Type `help <command>` at the FTP command line for a quick summary of the syntax for the command or consult the online help.

File already exists.

File transfer to the client was unsuccessful because the **If File Exists** file transfer mode is set to **Cancel** and a file with the same name as the server file already exists on the local computer.

Out of memory.

There is not enough memory on the local computer. Close other open Windows applications and try again.

Session timed out.

After you are connected to a server, the client waits up to <n> seconds for data packets being transferred to or from the host. If nothing is received within the period specified, this timeout error appears; in this case, try the operation again. If you have received repeated timeout errors, increase the session timeout value. To do this open the **Connection** tab, and edit the **Session** text box under **Timeout in seconds**, or use `SET TIMEOUT-SESSION` at the command line. (Connection timeouts are governed by a separate **Connect** text box).

Server response time can be affected by the distance between sites. Specifying a higher value gives the server more time to respond.

Unknown command <command>. Type 'help' for a list of valid commands.

Command line error. The command you entered is not recognized. Type `help`at the FTP command line for a list of the available FTP commands, type `help <command>` for a summary of the syntax for a specific command, or see the Command Reference topic.

502 PASV command not implemented by this server

If you receive an error message saying that PASV is not implemented by the server, you should disable the **Use passive mode** setting, which is enabled by default. This setting supports connections through some firewalls.

Related Topics

- "Connect to a Site" on page 775

Windows Sockets Error Messages

Following is a list of the Windows Sockets error messages that may appear during a Reflection FTP Client session and an explanation of how to resolve the error condition. These error messages (which are all preceded by the identifying string "WINSOCK error:") are returned by the Windows Sockets library if an error occurs in the network interface layer between Windows and the TCP/IP stack you are using. The Windows Sockets library (supplied in a module called Wsock32.dll) is included as part of the Windows operating system.

For some network Windows Sockets implementations, when you are connected to a server, several things can cause this message to be displayed:

- You tried to start a file transfer or perform a directory operation (such as changing directories or refreshing the current directory). If you see this error when attempting to transfer a file or to obtain a directory listing, then your network implementation does not work with the FTP Client.

- You started another instance of the FTP Client and tried to open another connection to the same server. If you get this error message when trying to connect, it indicates that your network implementation supports only one connection at a time to a given server. You cannot start separate instances of the FTP Client and attempt to connect to the same server with each instance.

Connection refused

The connection attempt was unsuccessful due to a problem on the host; possibly the host is down or the server is not running at this time. Wait a while, and then try to connect again.

Connection reset by peer

During a file transfer, the remote host reset the server connection. Close the server connection, reconnect, and try the transfer again.

Connection timed out

The attempt to connect to a server was timed out by your network software without establishing a connection. This may be because the server is not running. Wait a while, and then try to connect again.

Network is down

The Windows Sockets implementation has detected that the network subsystem has failed. Your network should be restarted.

Network is unreachable

The network can't be reached from this host at this time. This error can occur when you use an IP router (gateway) to connect to servers outside your own network. The message indicates that one of the IP routers along the path from your gateway to the destination networks is down. Contact your system administrator, who can check the hops between your gateway and the destination network.

No buffer space available

There are too many open connections. This error condition can occur when opening a connection to a server or transferring a file, or when the client requests server directory information. Close other open server connections or applications that use Windows Sockets and try the operation again. Check your network documentation for information about how to increase the buffer space for which your network is configured.

Operation not supported on socket

The client must open a data session prior to performing a file transfer or directory listing operation. A data session can't be opened using your network's Windows Sockets implementation.

Software caused connection abort

While transferring files to or from the server, the virtual circuit used for the server connection was aborted due to a timeout or other failure (possibly the host went down, or the FTP or SFTP server is not running). Close the server connection, reconnect, and try the transfer again.

Too many open files

To solve this problem, exit Windows, increase the `Files=` setting in your `Config.sys` file and reboot your PC. If you still get this message, try closing other open client sessions and then try to open the connection again. If your problem is still unresolved, contact the manufacturer of your Wsock32.dll for help.

Related Topics

 ◆ "FTP Client Error messages" on page 834

Error Messages

Click on an error message to view details.

Could not resolve host address.

Several things can cause this message to appear:

 ◆ The host name or IP address you entered for the server is invalid. Re-enter the host name; if you are connecting to a case-sensitive server, be sure to use the correct case.

 ◆ The host name you provide is resolved via the HOSTS file or a domain name server. Is the computer that acts as the domain name server working? Has the HOSTS file on your PC been corrupted? If no domain name server or HOSTS file is available, you must specify the full IP address of the host server. For example: 124.24.36.85.

 ◆ You have entered an IPv6 address, but have not enabled IPv6 support on your PC. Contact Microsoft for more information.

 ◆ You must have an appropriately configured IP router (gateway) in order to connect to servers outside your own network. Check to see whether the computer serving as the router is up and running.

Connection timed out.

Server response time can be affected by the distance between sites. If you see this message when trying to connect to a server, increase the **Connect Timeout** setting to give the server more time to respond during the login process.

Reflection FTP hangs when you try to connect

On some systems, turning off the use of animation (such as showing a waving flashlight while you are waiting for a directory listing) fixes display problems that cause Reflection to hang when you attempt a connection. To disable the use of animation, open the **Tools** menu, click **Options**, open the **Preferences** tab and enable **Do not use animation**.

Host cannot respond to the PWD command

By default, Reflection sends a PWD command when you connect to your server. Some servers don't support this command. Press F7 to open the command window before you try connecting to your server. If the server returns an error after Reflection sends the PWD command, try enabling this setting. To configure Reflection to connect without the PWD command, open the **Directories** tab of the **Site Properties** dialog box and select **Don't send PWD Command**.

PASV is not implemented by the server

By default, the client connects using the PASV command. This causes the client to initiate a separate data connection for directory listings and file transfers, which is required for connections through some firewalls. If your server does not support the PASV command, you can disable the **Use passive mode setting** on the **Connection** tab of the **Site Properties** dialog box.

Server returns error "425 can't establish data connection"

If you don't see a directory listing in either the server pane or the command window, your server may not support the PASV command. Try clearing the **Use passive mode** setting in the **Connection** tab of the **Site Properties** dialog box.

System cannot find the path

This error may indicate that the FTP Client is trying to find a local file path that does not exist. Check the local **Home** folder setting to be sure that the folder path exists on your computer. To view or edit this setting, open the **Site Properties** dialog box, click **Directories**, then find **Home folder** under **Local**.

Using the FTP Command Window

In this Section

The FTP Command Window

The FTP Client command window shows the data sent to and from the server and also includes the FTP Command line, which you can use to enter FTP or SFTP commands. Use **View**> **Command Window** to show or hide the command window.

An identifying color is assigned to each type of client/server communication that displays in the window. For example, if you are using the Windows default color scheme:

Color of text	Meaning
black	A command status message received from the server (command status messages are the server's responses to FTP or SFTP commands issued by the client)
royal blue	A Reflection FTP or SFTP command entered at the FTP command line
dark blue	A data channel response from the server, generally a file listing. After a connection is made, this color is also used to display the presumed server type.
green	A client FTP or SFTP command that the FTP Client is sending to the server
red	An error message

NOTE

- If the window background for your current Windows color scheme is set to blue, green, black, or red, the client changes the identifying colors used in the datacomm display window to ensure that text is visible against the window background. The display color for messages received from the server defaults to the color of window text in your current Windows color scheme.

- If you are connected to two sites in the same FTP Client window, you can use the command line to view communication between the client and the server, but you cannot enter commands. Commands sent to and from the second server are preceded by this identifier: **[Server 2].** If there is more than one line of output (such as directory listings and multi-line banners), only the first line has this identifier.

Related Topics

- "Use the FTP Command Line" on page 839
- "Clear the Command Window" on page 839
- "FTP and SFTP Command Syntax" on page 840
- "Command Reference" on page 848

Clear the Command Window

To clear the FTP Client command window

1 In the Command window, click the right mouse button and select **Clear All**.

Related Topics

- "The FTP Command Window" on page 838

Use the FTP Command Line

The FTP Client command line provides an alternate way for you to communicate with the server. You can enter FTP or SFTP commands on the FTP command line to move files between the FTP server and your PC.

To show or hide the FTP command line

◆ From the **View** menu, choose **Command Window** to toggle the command window display.

 The FTP command line appears at the bottom of the command window.

To enter commands

1 Click in the command line or press Shift+F7 to move the cursor to the command line.

2 Enter an FTP or SFTP command, depending on your connection type.

3 Press the Enterkey to execute the command.

The FTP Client keeps a list of up to 50 commands from the current session. You can use the drop-down arrow on the right side of the command line to recall items from this list.

NOTE: If you are connected to two sites in the same FTP Client window, you can use the command line to view communication between the client and the server, but you cannot enter commands. Commands sent to and from the second server are preceded by this identifier: **[Server 2]**. If there is more than one line of output (such as directory listings and multi-line banners), only the first line has this identifier.

Related Topics

FTP and SFTP Command Syntax

Case is not important for commands and keywords entered at the FTP command line. Depending on your FTP server computer, however, passwords, directory names, filenames, and other server-specific information may be case sensitive.

The FTP Client accepts abbreviated versions of commands, requiring that you type only as much of the command keyword as is necessary to make it unique. For example, the `GET` command can be abbreviated to G; to get the server file `jokes.old` you could enter `g jokes.old` at the FTP command line.

In the command references in this guide, the following conventions apply:

◆ When parameters are enclosed in angle brackets, they represent a string that must be added to complete the command. For example, `<clientfile>` means you must give a complete path to clearly reference a particular file. Do not include the brackets when entering the parameter.

- A vertical bar separates mutually exclusive options. For example, `<servername> | <ip address>` means you may use either of the options, but not both.

- Parameters enclosed in square brackets indicate optional components of a command; that is, any information contained within a pair of such brackets can, but need not, be included in the command. For example, the following indicates that the LCD command can be used with or without a PC directory:

  `lcd [<pc directory>]`

Related Topics

Quotation Marks in FTP or SFTP Commands

If a command takes only one argument, no quotation marks are required. For example:

`CD Travel Agents`

With commands that take more than one argument, any argument that contains spaces must be enclosed in double quotation marks. For example, to transfer the server file `Account History` to the PC and name it `Accthist.txt`, you would enter this command:

`GET "Account History" TO Accthist.txt`

If an argument begins with a double quotation mark, all double quotation marks in the argument must be doubled. For example, to transfer the server file `"Remembering You"`, you would enter a command in this format:

`GET ""Remembering You""`

FTP Scripting

Related Topics

In this Section

- "Commands for Error Handling" page - "Running a Script as a Background Task" on page 847
- "Creating Script Log Files" on page 847

FTP Client Scripting

FTP Client scripts allow you to automate connection and file transfer operations. For example, you can automate file transfers to and from a server. Automated transfers can be carried out without the need to interact directly with the FTP Client.

A script file is an ASCII text file that contains a sequence of FTP (or SFTP) commands. Each command must be on a separate line. You can create a script using the Script Recorder. You can also create a new script or modify an existing script using a text editor (such as Notepad).

Use the FTP Client script recorder to record actions as commands—you do not have to do any writing or programming to create a script that can be played back later. Scripts can automate many sorts of tasks (for example, configuring file transfer options, connecting to an FTP site, or transferring files).

When you play back a script, commands are executed as though they had been entered at the FTP command line.

Related Topics

- "Record a Script" on page 842
- "Run a Script" on page 843
- "Edit a Script" on page 843
- "FTP Client Script File Format" on page 843

Record a Script

Use the FTP Client script recorder to record actions as commands—you do not have to do any writing or programming to create a script that can be played back later. Scripts can automate many sorts of tasks (for example, configuring file transfer options, connecting to an FTP site, or transferring files).

To record a script

1 From the **Script** menu, choose **Start Recording**.

  When the script recorder is active, a camera icon appears in the status bar.

2 Perform the actions you want to record.

3 From the **Script** menu, choose **Stop Recording**.

4 In the **Save Script** dialog box, type a name for the script in the **File name** box.

  The default extension for script files is `.rfs`.

5 Click **Save**.

NOTE: You cannot record scripts when you are connected to two sites in the same session.

Related Topics

Run a Script

1 From the **Script** menu, choose **Run Script**.

2 In the **Run Script** dialog box, select the script you want to run.

3 Click **Open** to play back the selected script.

Related Topics

Edit a Script

1 From the **Script** menu, choose **Edit Script**.

2 In the **Edit Script** dialog box, select the script you want to edit.

3 Click **Open** to open the file in Notepad.

Related Topics

FTP Client Script File Format

A script file is an ASCII text file that contains a sequence of FTP (or SFTP) commands.

- Each command must be on a separate line.
- Space and tab characters can precede the command on a line.
- Use a semicolon character (;) for comments. The FTP Client ignores comment text.

You can use comments to explain one or more lines of code. For example:

```
;The following lines connect to the server and change
;the working directories to PREPRESS (client) and
;PRESS (server).
open forum thomasp XOYRCNEL973L9L96O376ONMO770L35L7NMO87PM79
lcd c:\prepress
cd /press
```

You can also add a comment at the end of a command. For example:

```
set transfer-disposition unique  ;do not overwrite files
mput script is s*.doc  ;copy the .DOC files
```

NOTE: Semicolons are not supported for comments in scripts supplied to the **sftp** command line using the **-B** option. Use the number sign (#) to mark comments in these batch files.

Related Topics

Which Actions Are Captured by the Script Recorder?

Most connection and file transfer operations you perform while the script recorder is on are recorded, but there are some exceptions: configuration options that you change via the graphical user interface are not recorded. To include file transfer and character translation configuration settings in a recorded script, enter SETparameters at the command line or edit the script to add SETparameters.

NOTE: You cannot record scripts when you are connected to two sites in the same session.

The following actions generate FTP script commands that are recorded:

- All commands entered in the command window are recorded.
- File operations you perform using the graphical user interface (GUI). See the following table to see which FTP commands are recorded.

FTP Command	GUI Action That Generated It
OPEN	Opening an FTP Site (**Open** toolbar button or menu).
CLOSE	Closing an FTP Site.
CD	Clicking on a folder in the Site pane (or using **Go to** dialog box).
LCD	Clicking on a folder in the Local pane.
DELETE*	Deleting a file in the Site pane.
LDEL*	Deleting a file in the Local pane.
RDALL*	Deleting a folder in the Site pane.
LRDALL*	Deleting a folder in the Local pane.
MD	Creating a folder in the Site pane.
LMD	Creating a folder in the Local pane.
GET*	Dragging a file from the Site pane to the Local pane.

FTP Command	GUI Action That Generated It
\<None\>	Dragging a file from the Site pane to Windows Explorer, the desktop, or a My Computer folder.
CPDIR*	Dragging a folder from the Site pane to the Local pane.
\<None\>	Dragging a folder from the Site pane to Windows Explorer, the desktop, or a My Computer folder.
PUT*	Dragging a file from the Local pane to the Site pane.
PUT*	Dragging a file to the Site pane from Windows Explorer, the desktop, or a My Computer folder.
LCPDIR*	Dragging a folder from the Local pane to the Site pane.
LCPDIR*	Dragging a folder to the Site pane from Windows Explorer, the desktop, or a My Computer folder.

* Multiple selection invokes this FTP Command multiple times.

NOTE

- If you enter an `open <servername> <username> <password>` command, the `<password>`is saved as obfuscated text in the script file. For example:

```
open ftp.myco.com joe WPD6119O0O3929K148O6KN70652L0739LL00875N44O274
```

- If the server returns an error message when a command is entered, that error message is recorded as a comment line in the script. For example:

```
cd /users/bobc
; 550 /users/bobc: No such file or directory.
```

Related Topics

Password Security within Scripts

Passwords can be included in scripts for establishing FTP (but not SFTP) connections. When you write a script in a text editor, if the script includes a complete **OPEN** command (`open <servername> <username> <password>`), or includes a **PASSTHRU** command, passwords you add manually will be visible in the editor as plain text. For greater password security use one of these methods:

- Use the Script Recorder to record the connection to the server. Passwords are stored as obfuscated text in the script file. When the script runs and a connection is opened, the client deciphers the password and sends it to the server.

- Edit the script to remove the `<password>` parameter, which is the last parameter in the **OPEN** command. The **OPEN** command should have the format: `open <servername> <username>`. When the script runs and a connection is opened, the client prompts the user for a password. You may also want to omit the `<username>` parameter, which causes the client to prompt for both the user name and the password.

Related Topics

-
-
-
-

Commands for Error Handling

Include a **CONTINUE** command in your script file to tell the FTP Client how to handle errors that occur when you are using wildcards to transfer files or delete local files. When **CONTINUE** is `ON`, file transfers or local file deletes proceed until all files satisfying the wildcard specification have been transferred or deleted, even when an error occurs. When **CONTINUE** is `OFF`, the transfer or delete operation aborts if an error occurs during the process; the script file terminates in response to the error, unless **ABORT-ON-ERROR** is set to `NO`.

The **ABORT-ON-ERROR** parameter specifies whether execution of a script stops whenever an error occurs in response to a command. When **ABORT-ON-ERROR** is set to `YES`, script execution will terminate any time a command results in an error response from the FTP Client or server.

Use caution when setting **ABORT-ON-ERROR** to `NO`. Continuing command execution after an error can yield unexpected results.

Related Topics

-
-
-
-

Running a Script as a Background Task

You can create a script and configure the FTP Client so that, when the script executes, the client runs as a background task and there is no interaction or communication with the user. To do so:

- Create a shortcut with a startup command that automatically executes the script. In the **Run** box, select **Minimized** to specify that the FTP Client should run minimized on the desktop.
- Have the script connect to a site for which you already have saved the user name and password and any passthrough settings needed to connect to that site. This prevents the client from prompting for connection information.
- Include a **QUIT** command to have the client shut down when the script completes.
- Use the following **SET** parameters to control the client display of messages and prompts:

Setting	Usage
QUIET-STATUS	Set to YES to suppress the connection and transfer progress dialog boxes and the Directory Definition Wizard.
SMART-TYPE-DEFAULT	Do not set to ASKUSER. When set to ASKUSER, the user is prompted for a transfer method if the script transfers an unrecognized file type.
TRANSFER-DISPOSITION	Do not set to PROMPT. When set to PROMPT, the user is prompted during transfer to specify handling for files that exist at the destination.
CONFIRM-DELETE	Set to NO to prevent the client from prompting for confirmation prior to deleting files or folders.
RESUME-PARTIAL-TRANSFERS	Do not set to ASKUSER. When set to ASKUSER, the user is prompted to choose whether to resume a partial transfer if the FTP Client detects that a prior incomplete server file download occurred.

Related Topics

- "Run a Script" on page 843
- "Save your FTP Client Settings" on page 788
- "Create a Shortcut to Connect to a Site" on page 825
- "FTP Client Startup Switches" on page 825
- "Run a Script File at Startup" on page 827
- "SET" on page 894

Creating Script Log Files

When you start the FTP Client with a startup command that executes a script file, you can include a command line switch that directs the client to create a log file that stores a record of the results of the commands that are executed.

If you want to create a log file when you execute a script file from within the client application, from the **Tools** menu, choose **Start Logging**, and then, from the **Script** menu, choose **Run Script**.

If you are using the FTP Automation API to control the FTP Client application, you can control logging using the **StartLog** and **StopLog** methods.

Related Topics

- "FTP Client Startup Switches" on page 825
- "Run a Script File at Startup" on page 827
- "Options for Automating FTP Client Transfers" on page 774

Command Reference

The commands available to you for use on the command line and in scripts depend on which kind of connection you have made.

TIP: When you open a command topic, you can tell if it is available with FTP, SFTP, or both by looking to see which list or lists are linked to at the top of the topic.

In this Section

- "FTP commands" on page 848
- "SFTP commands" on page 883

FTP commands

You can use the commands in this list on the FTP Client command line or in a script. (If you have made a Secure Shell SFTP connection, use the "SFTP commands" on page 883 instead of the commands in this list.) Use the following links to view additional command reference information.

In this Section

- "ACCOUNT" on page 850
- "APPEND" on page 850
- "ASCII" on page 850
- "BINARY" on page 851
- "CD" on page 851
- "CHMOD" on page 851
- "CLOSE" on page 852
- "CONNECT" on page 852
- "CONTINUE" on page 852
- "CPDIR" on page 853
- "DELETE" on page 853
- "DIR" on page 854
- "DISCONNECT" on page 854
- "DISPLAY" on page 854

ACCOUNT

Syntax: `account <accountname>`

Some servers (for example, some IBM FTP servers) require the name of the account that the user wants to access. For servers with this requirement, you cannot work with the files in that account until you supply an account name. If you connect using an "OPEN" on page 863 command that includes an `<account>` parameter, the account name is not actually sent to the server unless the server specifically prompts for an account during the login. If your server requires an account name, but doesn't request that name during the login process, use the **ACCOUNT** command to explicitly tell the server which account you want to use.

`<accountname>`	Specifies an account that the logged in user has rights to access. For case-sensitive servers, be sure to use the appropriate case when typing the account name.

APPEND

Syntax: `append <clientfile> [to] [<serverfile>]`

The **APPEND** command sends a file to the FTP server, appending it to the current server file. If the server file does not exist, this command creates it, and works exactly like the "PUT" on page 865 command.

`<clientfile>`	Specifies the PC file to transfer to the FTP server.
`to <serverfile>`	Specifies the server file to which the PC file should be appended. If this option is omitted, the PC file is appended to a server file having the same name as the PC file. If the specified server file does not exist, it is created. The TO keyword is optional.

Examples

The following command appends a PC file to a server file of the same name:

`APPEND WHATSNEW.DOC`

This command appends a PC file to the specified server file:

`APPEND WHATSNEW.DOC TO DOCUMENT.TXT`

ASCII

Syntax: `ascii`

The **ASCII** command changes the current file transfer method to ASCII. Use this transfer method to move ASCII text files between the server and your PC.

BINARY

Syntax: `binary`

The **BINARY** command changes the current file transfer method to binary (image). Use this transfer method to transfer binary files, such as .EXE files and compressed files, between two PCs (via a server), or between two servers (via a PC).

CD

Syntax: `cd <server directory>`

The **CD** command changes the working directory on the FTP server.

`<server directory>`	Specifies a directory on the server.

Examples

This command changes to the directory "Asian Artists" on a UNIX system:

```
CD Asian Artists
```

This command changes directories on a VAX/VMS system:

```
CD SYS$USERS:[ARNOLD.DOCS]
```

CHMOD

Syntax: `chmod <numeric permission mask> <server file or directory>`

The **CHMOD** command changes the permissions associated with a file or directory.

`<numeric permission mask>`	Specifies a three digit numeral that is a valid value for the UNIX chmod command. Valid values have digits from 0 to 7.
	Tip: To determine what mask to use to set permissions, right click on a server file and select properties. The properties dialog box displays the three digit mask and the permissions associated with it. If you change the permissions, the mask value is updated automatically.
`<server file or directory>`	Specifies a file or directory on the FTP server. Follow the server's syntax for specifying file and directory names.

Example

This command sets attributes to `-rw-r--r--` for the specified file.

```
chmod 644 myfile.htm
```

CLOSE

Syntax: `close`

The **CLOSE**command closes the connection to the FTP server.

You can also use **EXIT** or **QUIT** as a synonym for **CLOSE**.

CONNECT

Syntax: `connect [<servername>]`

The **CONNECT**command initiates a connection to an FTP server. If no site is specified, a dialog box will prompt for this information. Unlike "OPEN" on page 863, this command does not prompt for user name and password. This information must be entered manually. For example, the following command sequence would connect you to an FTP server that does not use a passthrough server (firewall):

```
CONNECT <server>
USER <username>
PASS <password>
```

Note that passwords appear as text on screen when you enter them directly in the command window. Because the **OPEN** command prompts for passwords with dialog boxes that do not display password text, this command is preferable for most connections. Use **CONNECT**if you are troubleshooting connections through a firewall.

CONTINUE

Syntax: `continue [on | off]`

The **CONTINUE**command instructs Reflection FTP to ignore errors that occur during a wildcard file transfer initiated at the FTP command line. File transfer proceed as though no error occurred, until all files satisfying the wildcard specification have been transferred.

CONTINUEwith no arguments tells Reflection FTP to ignore an error in the next "MGET" on page 860 or "MPUT" on page 862 command only.

The **CONTINUE**command only applies to the series of commands that comprise an MGET or **MPUT**block (such as **LIST, GET, PUT, CD**). If an error is encountered in any of the commands in the series, the script will stop after it finishes the complete **MGET**or **MPUT**command series. To allow the script to process further commands, change **SET-ABORT-ON-ERROR** (page 869) to NO.

The **CONTINUE**command does not apply to drag-and-drop file operations.

`on`	Tells Reflection to ignore all file transfer errors, as if every subsequent **MGET**and **MPUT**command were preceded by a **CONTINUE**.
`off`	Reverses the ON option.

Example

This sequence of commands instructs Reflection FTP to ignore any error in the next **MPUT**command. Without **CONTINUE,**the **MPUT**command aborts if an error occurs during the transfer.

```
CONTINUE
MPUT ACCT*.TXT
```

See for an additional example.

CPDIR

Syntax: `cpdir <server directory> [<pc-path>] [askuser | cancel | overwrite | skip]`

The **CPDIR**command copies the specified server directory to the PC. If a PC directory is not specified, the server directory is copied to the current PC path.

`server directory`	Specifies the name of the server directory.
`pc-path`	Specifies the PC drive and folder.
`askuser	cancel	overwrite	skip`	Specifies what to do if the target folder already exists. ASKUSER is the default.

DELETE

Syntax: `delete <serverfile>`

The **DELETE**command deletes a file matching the given filespec on the FTP server.

NOTE: If the **SET** parameter (page 869) CONFIRM-DELETE is set to YES, the user is prompted for confirmation before deleting.

`<serverfile>`	Specifies the name of a server file to delete. This can include a full directory path to the file. On some systems such as UNIX FTP servers, case is important when specifying directories and file names.

Examples

This command deletes MEMO.DOC from the current server directory:

```
DELETE MEMO.DOC
```

The next command deletes the budget.new file from the /users/jill jones directory on a UNIX FTP server:

```
DELETE /users/jill jones/budget.new
```

DIR

Syntax: `dir [<server filespec>]`

The **DIR**command displays a detailed listing of server files matching the given file specification. (Compare this to the command, which displays a less detailed listing.)

`<server filespec>`	Specifies a directory, file, or group of files on the FTP server. If this option is not used, the contents of the current server directory are displayed. The syntax for <server filespec> varies according to your FTP server.

Example

This command displays a list of executable files in the current directory on a VAX/VMS FTP server:

`DIR *.EXE`

DISCONNECT

Syntax: `disconnect`

The **DISCONNECT**command closes the connection to the FTP server.

You can also use **CLOSE**, **EXIT**, or **QUIT** as a synonym for **DISCONNECT**.

DISPLAY

Syntax: `display <string>`

The **DISPLAY**command displays data in the command window as if it had been received from the FTP server.

`<string>`	The `<string>` parameter can be any string of characters.
	The character string displays on a single line. If the specified character string exceeds the width of the Reflection FTP window, characters at the end of the string will be hidden; the string will not wrap to the next line. For example, if the window is sized to 50 columns wide and the `<string>` is 60 characters long, the last 10 characters of the string will be hidden.

Example

You can use the **DISPLAY** command to do such things as display a message or reminder about the current process. For example, the following command displays a message that a logon process occurs next:

`DISPLAY Next process is logon to bigben.timer.london`

EXIT

Syntax: `exit`

FTP Command Index (page 848)   SFTP Command Index (page 883)

The **EXIT**command closes the connection to the server.

GET

Syntax: `get <serverfile> [to] [<clientfile>] [append | askuser | cancel | overwrite | skip | unique]`

FTP Command Index (page 848)   SFTP Command Index (page 883)

The **GET**command transfers a file from the server to the PC. Wildcards are not supported with the **GET**command—they are treated as ordinary characters and are assumed to be part of the file name. To transfer multiple files, use "MGET" on page 860.

Before using the **GET**command, if necessary, use the "ASCII" on page 884, "BINARY" on page 851, "TENEX" on page 895, or "SMART" on page 894 command to override the default file transfer method setting specified on the **Tools** menu.

A variety of site-specific **SET**parameters can affect the transfer operation. Click here (page 879) for more information.

`<serverfile>`	Specifies the name of the server file.
`to <clientfile>`	Specifies the name of the PC file to be created. If this option is omitted, the client file receives the same name as the server file. The TO keyword is optional.
`append | askuser | cancel | overwrite | skip | unique`	Specifies what to do if the destination file already exists. If this option is omitted, the active **TRANSFER-DISPOSITION** (page 869) setting is the default.

Examples

The following example transfers the server file MEMO.DOC from the server to the PC, giving the PC file the same name:

`GET MEMO.DOC`

This example transfers the VAX/VMS FTP server file MORTGAGE.PAPERS to the PC, giving the PC file the name MORTGAGE.TXT:

`GET MORTGAGE.PAPERS MORTGAGE.TXT`

HELP

Syntax: `help [<command>]`

FTP Command Index (page 848)

HELPdisplays a short summary of FTP commands. You can type `HELP <command>` at the FTP command line to see information on a specific FTP command. For a listing of FTP commands without descriptions, enter HELP at the command line.

With many FTP servers, you can enter `QUOTE HELP` at the command line for a list of commands the server recognizes. Entering `QUOTE HELP <command>` sometimes gives more detailed information about the command. See "QUOTE" on page 866 for more information.

NOTE: HELPdisplays the FTP command list even if you have made an SFTP connection. Click here (page 883) for a list of commands available during SFTP sessions.

LCD

Syntax: `lcd [<pc drive/folder> | ..]`

The **LCD** command opens another folder on the PC.

If no `<folder>` is specified, **LCD** displays the path for the current PC folder.

To change folders, type the folder at the FTP command line, for example, type `LCD F:\Documents`and press Return.

`<pc drive/folder>`	Specifies the drive (if other than the current drive) and folder to change to.
`..`	Specifies that you want to change to the parent folder.

Example

This command changes your current folder to the China folder within the Asian Travel folder on drive D:

`LCD d:\Asian Travel\China`

LCPDIR

Syntax: `lcpdir <pc drive/folder> [<server folder>] [askuser | cancel | overwrite | skip]`

The **LCPDIR** command copies the specified PC folder to the server. If a server folder is not specified, the PC folder is copied to the current server path.

`pc drive/folder`	Specifies the local folder. Use quotation marks if the file or path includes spaces. For example: `lcpdir "d:\Asian Travel\China"`
`<server folder>`	Specifies the server folder.
`askuser	cancel	overwrite	skip`	Specifies what to do if the target folder on the server already exists. ASKUSER is the default.

LDEL

Syntax: `ldel <pc filespec>`

The **LDEL**command deletes the specified file on the PC. Wildcards are not supported.

NOTE: If the **SET** parameter (page 869) CONFIRM-DELETE is set to YES, the user is prompted for confirmation before deleting.

`<pc filespec>`   Specifies the name of a PC file to delete. The filespec can include a full directory path to the file.

Example

This command deletes Map.bmp from the France folder within the European Travel folder on the PC:

`LDEL \European Travel\France\map.bmp`

LDIR

Syntax: `ldir [<pc filespec>]`

The **LDIR**command displays a listing of PC files matching the given filespec.

`<pc filespec>`   Specifies a folder, a file, or a group of files on the PC. If this option is not used, the contents of the current PC folder are displayed.

Example

This command displays a listing of all the files in the specified PC folder that have the name Old Data and end with any extension:

`LDIR D:\Results\Old Data.*`

LMD

Syntax: `lmd <pc directory>`

The **LMD**command creates a folder on the PC.

`<pc folder>`   Specifies the drive where you want to create the folder (if other than the current drive) and the folder name.

Example

This command creates the folder Music on the current PC drive:

```
LMD \Music
```

LRD

Syntax: `lrd <pc directory>`

FTP Command Index (page 848)

The **LRD**command deletes a PC folder and all the files and folders it contains.

You can also use **LRDALL** as a synonym for **LRD**.

NOTE: If the **SET** parameter (page 869) CONFIRM-DELETE is set to YES, the user is prompted for confirmation before deleting.

`<pc folder>`	Specifies the location and name of the folder you want to delete. The <folder> specification must follow PC conventions

Example

This command deletes the folder "Trial Dates" from within the "Cases" folder on the J drive:

```
LRD J:\Cases\Trial Dates
```

LRDALL

Syntax: `lrdall <pc folder>`

FTP Command Index (page 848)

The **LRDALL**command deletes a PC folder and all the files and folders it contains.

You can also use **LRD** as a synonym for **LRDALL**.

NOTE: If the **SET** parameter (page 869) CONFIRM-DELETE is set to YES, the user is prompted for confirmation before deleting.

`<pc folder>`	Specifies the location and name of the folder you want to delete.

Example

This command deletes the folder "Trial Dates" from within the "Cases" folder on the J drive:

```
LRD J:\Cases\Trial Dates
```

LRENAME

```
lrename <pc filename> <new filename>
```

FTP Command Index (page 848)

The **LRENAME**command changes the name of a local file to the new name specified.

`<pc filename>`	Specifies the name of the PC file you want to rename. The specification can include the PC drive and folder where the file is located. If the file location or name contains spaces, the specification must be enclosed with quotation marks. For example: `"D:\To do\Monthly tasks"`.
`<new filename>`	Specifies the name you want to give the file. If the file to be renamed does not exist on the active local drive and folder, you must include the location in the `<new filename>` specification. Use quotation marks if the file or path includes spaces. For example, `"D:\To do\Work assignments"`.

Example

From the current folder on the C drive , this command renames a file in the folder "Archive" on the D drive, changing the name from "Stories.txt" to "Fairy tales":

`LRENAME D:\Archive\Stories.txt "D:\Archive\Fairy tales"`

LS

Syntax: `ls [<server filespec>]`

The **LS** command displays a simple listing of server files matching the given filespec. (Compare this to the command, which displays a more detailed listing.)

`<server filespec>`	Specifies a folder, file, or group of files on the server. If this option is not used, the contents of the current server folder are displayed.

Example

In this example, the names of all files in the current folder on a UNIX FTP server are listed:

`LS *.*`

LTYPE

Syntax: `ltype <clientfile>`

The **LTYPE** command displays the contents of a PC file in the FTP command window.

`<clientfile>`	Specifies the location and name of the PC file. This specification cannot contain wildcards.

Example

The following command displays the content of the file Com.doc in the Subjects folder on the J drive on the PC:

`LTYPE J:\Subjects\Com.doc`

MD

Syntax: `md <server folder>`

The **MD**command creates a folder on the server.

`<server folder>`   Specifies the name and location of the new folder.

Example

This command creates the folder Films within the current folder on the current FTP UNIX server drive:

`MD Films`

MDEL

Syntax: `mdel <server filespec>`

The **MDEL**command deletes one or more files matching the given filespec on the FTP server.

MDELdiffers from "DELETE" on page 853 in that **MDEL**supports multiple file deletions from the server using server wildcard characters. Your FTP server must support wildcards for multiple file deletions.

NOTE: If the **SET** parameter (page 869) CONFIRM-DELETE is set to YES, the user is prompted for confirmation before deleting.

`<server filespec>`   Specifies one server file or (using server wildcards) multiple server files. This can include a full directory path to the file. On some systems such as UNIX FTP servers, case is important when specifying directories and file names.

Examples

This command deletes all files from the current server directory:

`MDEL *`

This command deletes all files ending with ".htm" from the current server directory:

`MDEL *.htm`

See "ABORT-ON-ERROR Script Sample" on page 881 for an example.

MGET

Syntax: `mget <server filespec> [to] [<pc filespec>] [append | askuser | cancel | overwrite | skip | unique]`

The **MGET** command transfers one or more files matching the given filespec from the FTP server to the PC. You can use wildcards to transfer multiple files. Most servers support wildcards in the `<serverspec>`. However, if your server doesn't support wildcards in an "LS" on page 888 command, using **MGET** with a wildcard specification may result in a transfer of all files in the current directory.

NOTE: The Reflection client supports **MGET** in SFTP sessions, however you should test transfers that use wildcard characters because the SFTP server may not interpret wildcard specifications correctly.

Before using the **MGET** command, if necessary, use the "ASCII" on page 884, "BINARY" on page 851, "TENEX" on page 895, or "SMART" on page 894 command to override the default file transfer method setting specified on the Tools menu.

A variety of site-specific **SET** parameters can affect the transfer operation. Click here (page 879) for more information.

`<server filespec>`	Specifies one server file or (using server wildcards) multiple server files to transfer to the PC. If a `<server filespec>`is given with no other options, the PC files are given the same names as the server files.
`to <pc filespec>`	Specifies a PC folder to receive the files, or the name of the PC file to create. The TO keyword is optional. If this option is omitted, server files are transferred to the current folder.
	If `<server filespec>` specifies more than one file, the `<pc filespec>` should typically be a directory path. To consolidate a series of server files in one PC file, you can specify a file name for the `<pc filespec>` and use the APPEND option.
	Use quotation marks if the file or path includes spaces. For example:
	`MGET *.* "C:\My documents\*.*"`
`append | askuser | cancel | overwrite | skip | unique`	Specifies what to do if the destination file already exists. If this option is omitted, the active **TRANSFER-DISPOSITION** (page 869) setting is the default.

Examples

This example transfers all files with a .Doc extension from the FTP server to the PC, placing the files in the current PC directory:

`MGET *.Doc`

This example adds the letter A to the transferred files. For example, test.txt becomes Atest.txt.

`MGET *.* A*.*`

See "ABORT-ON-ERROR Script Sample" on page 881 for an additional example.

MPUT

Syntax: `mput <pc filespec> [to] [<server filespec>] [append | askuser | cancel | overwrite | skip | unique]`

The **MPUT**command transfers one or more files matching the given filespec from the PC to the FTP server. You can use wildcards to transfer multiple files.

NOTE: The Reflection client supports **MPUT** in SFTP sessions, however you should test transfers that use wildcard characters because the SFTP server may not interpret wildcard specifications correctly.

Before using the **MPUT** command, if necessary, use the "ASCII" on page 884, "BINARY" on page 851, "TENEX" on page 895, or "SMART" on page 894 command to override the default file transfer method setting specified on the **Tools** menu.

A variety of site-specific **SET** parameters can affect the transfer operation. Click here (page 879) for more information.

`<pc filespec>`	Specifies one PC file or (using wildcards) multiple PC files to transfer to the server. The files are placed in the current server directory and are given the same names as the PC files.
	PC wildcard characters (the ? and * characters) can be used to send multiple files to the server. For example, to send all files in the current directory with the file extension `.Txt`, use the command `MPUT *.Txt`.
	Use quotation marks if the file or path includes spaces. For example:
	`MPUT "C:\My documents\*.*"`
`to <server filespec>`	Specifies a server file or (using server wildcards) multiple server files to receive the PC files. If files of this name don't exist, they are created by the transfer. If no value for <server filespec> is given, server files are given the same name as the PC files.
	The TO keyword is optional.
`append	askuser	cancel	overwrite	skip	unique`	Specifies what to do if the destination file already exists. If this option is omitted, the active **TRANSFER-DISPOSITION** (page 869) setting is the default.

Examples

The following example transfers files in the Meeting Notes folder within the current folder on the PC that have a .Doc extension , placing the files in the current server folder. Source PC files that have the same name as files in the destination server folder are not transferred.

`MPUT "Meeting Notes\*.Doc" skip`

The following example adds the letter "A" to the front of files transferred to the server. For example Sample.htm becomes ASample.htm.

`MPUT *.htm A*.htm`

The final example removes file extensions from PC files copied to the server:

```
MPUT *.*  *.
```

OPEN

Syntax: `open [<servername> [<username> [<password> [<account>]]]]`

The **OPEN** command connects to the FTP server and attempts to log in using the server name, username, and password specified. For case-sensitive servers, be sure to use the appropriate case when typing parameter values. If no parameters are specified with the **OPEN** command, the user is prompted for login information.

When only one parameter is present, it must be `<servername>`. If you add a second parameter it must be `<username>`. If you use three parameters, the third must be `<password>`.

NOTE: If you use a passthrough server to log into FTP servers, use the command to open a server connection.

`<servername>`	Specifies a server. This can be an IP address, a URL, or a name from a Hosts file.
`<username>`	Specifies a valid username registered on the current FTP server. When opening an anonymous connection, the username is usually "anonymous."
`<password>`	Specifies the password assigned to user `<username>`. Most anonymous FTP servers expect you to supply your e-mail address as the password.
`<account>`	Specifies an account that user `<username>` has rights to access. Typically, anonymous FTP servers do not request an account, so this parameter can be omitted.
	When an **OPEN** command that includes an `<account>` parameter is executed, the account name is not sent to the server unless the server specifically prompts for an account during the login. If your server requires an account name, but doesn't request that name during the login process, use the "ACCOUNT" on page 850 command to explicitly tell the server which account you want to use.

Examples

This command opens an anonymous connection to the FTP server, supplying an e-mail address for the password:

```
OPEN ftp.acme.com anonymous jackie@mycompany.com
```

The following command opens a connection to the Headquarters FTP server for user Jackie. A password parameter wasn't specified, so the user will be prompted to enter a password during the login process.

```
OPEN Headquarters Jackie
```

PASSTHRU

Syntax 1: `passthru <passthrough servername> <username>@<servername> <password>`

Syntax 2: `passthru <passthrough servername> <passthrough username>`
  `<passthrough password> <username>@<servername> <password>`
Syntax 3: `passthru <passthrough servername> <passthrough username>`
  `<passthrough password> <servername> <username> <password>`

The **PASSTHRU**command opens a connection to the FTP server using the passthrough server specified. Two styles of passthrough servers are supported. Reflection FTP sends different commands to log into the passthrough server and connect to an FTP server, based on the **PASSTHRU**syntax you specify.

When using any form of the **PASSTHRU**command, all parameters are required. If you specify "" (a null value) for a parameter, the FTP Client displays a dialog box prompting for that value. For case-sensitive servers, be sure to use the appropriate case when typing parameter values.

NOTE: If the FTP server you connect to with the PASSTHRU command requires an account name, use the "ACCOUNT" on page 850 command to tell the FTP server which account you want to use.

Syntax 1

Use this type of **PASSTHRU**command if your passthrough server is a `username@servername` style server that does not require a passthrough password (that is, it does not perform authentication).

This form of the **PASSTHRU**command sends the current FTP server user name and server name in the format `username@servername` to the passthrough server specified in <passthrough servername>. The passthrough server uses this information to open a connection to the specified FTP server.

`<passthrough servername>`	Specifies a connection name for the passthrough server. If you want the FTP Client to prompt for the passthrough servername, specify "" (a null value) for this parameter.
`<username>@<servername>`	The `<username>` portion of the argument specifies a valid user name registered on the FTP server.
	The `<servername>` portion of the argument specifies a connection name for the FTP server.
`<password>`	Specifies the password assigned to user `<username>`on the FTP server. If you want the FTP Client to prompt for the user password, specify "" (a null value) for the password.

Syntax 2

Use this type of **PASSTHRU**command if your `username@servername` style passthrough server is set up to authenticate the user on the passthrough server prior to opening a connection to an FTP server.

This form of the **PASSTHRU** command allows you to log into a `<username@servername>` style passthrough server that will open the connection to the FTP server. The command logs into the passthrough server specified in < `passthrough servername`>. The login command provides the username and the password on the passthrough server, based on `<passthrough username>` and `<passthrough password>`. Once the user is authenticated on the passthrough server, the FTP `<username>` and FTP `<servername>` are sent to the passthrough

server. This information is specified in the format: `username@servername`. The passthrough server uses this information plus the FTP server `<password>` to open a connection to the FTP server.

Syntax 3

This form of the **PASSTHRU**command allows you to log into a SITE servername style passthrough server that will open the connection to the FTP server.

Reflection FTP sends a command to log into the passthrough server specified in `<passthrough servername>`. The login command provides the username and the password on the passthrough server, based on `<passthrough username>` and `<passthrough password>`. Once a connection is opened, a site command is sent to the passthrough server, passing the settings needed to connect to the FTP server (`<servername>`, `<username>`, and `<password>`). The passthrough server uses this information to open a connection to the FTP server.

PUT

Syntax: `put <clientfile> [to] [<serverfile>] [append | askuser | cancel | overwrite | skip | unique]`

The **PUT**command transfers a file from the PC to the server.

Wildcards are not supported with the **PUT**command; to transfer multiple files using wildcards, use "MPUT" on page 862.

Before using the **PUT**command, if necessary, use the "ASCII" on page 884, "BINARY" on page 851, "TENEX" on page 895, or "SMART" on page 894 command to override the default file transfer method setting specified on the **Tools** menu.

A variety of site-specific **SET**parameters can affect the transfer operation. Click here (page 879) for more information.

`<clientfile>`	Specifies the name of the PC file. Use quotation marks if the file or path includes spaces.
`to <serverfile>`	Specifies the name of the server file to be created. If the server file name is omitted, the server file is given the same name as the PC file. The TO keyword is optional.
`append | askuser | cancel | overwrite | skip | unique`	Specifies what to do if the destination file already exists. If this option is omitted, the active **TRANSFER-DISPOSITION** (page 869) setting is the default.

Examples

The following example transfers the file Memo.doc from the PC to the server:

`PUT Memo.doc`

This example transfers the file HAPPY.ME from a PC to a VAX/VMS FTP server, giving the VMS file the name HAPPY.BIRTHDAY:

`PUT HAPPY.ME TO HAPPY.BIRTHDAY`

See for an additional example.

PWD

Syntax: `pwd`

The **PWD**command shows the server folder that is currently open. The name and location of the folder display in the FTP command window.

QUIT

Syntax: `quit`

The **QUIT**command closes the connection to the server.

NOTE: When you run a script from the Windows command line using the /RFS switch and the script ends in with a **QUIT** command, the FTP client shuts down automatically when the script is complete.

QUOTE

Syntax: `quote <string>`

The **QUOTE**command sends a string to the FTP server. Use **QUOTE**to issue commands to the FTP server that are not implemented by the Reflection FTP Client.

With many FTP servers, you can type `QUOTE HELP` for a list of commands the server recognizes. Typing `QUOTE HELP <command>` sometimes gives more detailed information about the command.

`<string>`	Specifies the string to send to the server. Valid strings you can use with the **QUOTE** command depend entirely on the FTP server; check your server documentation for details.

Example

To create the subdirectory FIFE on a VAX/VMS FTP server, you could use this command:

`QUOTE MKD MAYBERRY$USERS:[BARNEY.FIFE]`

RD

Syntax: `rd <server folder>`

The **RD**command deletes an empty folder on the server.

Note: If the **SET** parameter (page 869) CONFIRM-DELETE is set to YES, the user is prompted for confirmation before deleting.

`<server folder>`	Specifies the location and name of the folder you want to delete. Before you can delete a folder, you must delete the files and folders within it.

Example

This command deletes the folder Articles from the current server folder:

`RD Articles`

RDALL

Syntax: `rdall <server folder>`

FTP Command Index (page 848)

The **RDALL** command deletes a folder and all the files and folders within it on the server.

NOTE: If the **SET** parameter (page 869) CONFIRM-DELETE is set to YES, the user is prompted for confirmation before deleting.

`<server directory>`	Specifies the location and name of the directory you want to delete. On some systems such as UNIX FTP servers, case is important when specifying directories.

Examples

This command deletes the directory Maps from the current server location:

`RDALL Maps`

This command deletes the folder "Destinations" from the "Travel/Europe" folder:

`RDALL /Travel/Europe/Destinations`

REGET

Syntax: `reget <serverfile> [to] [<clientfile>]`

FTP Command Index (page 848)

The **REGET** command directs the FTP Client to automatically resume an incomplete file transfer from the FTP server to the PC. The Client automatically completes the file transfer from the point at which the download was interrupted.

If the Client does not find a partial file locally, it performs a "GET" on page 855 to do a complete transfer of the specified server file. If the local folder already contains a file with the same name as the file being transferred, the local file is overwritten.

NOTE: The **REGET**command works only for BINARY file transfers. Before using the **REGET**command, if necessary, use the "BINARY" on page 851 command to override the default file transfer method setting specified on the **Tools** menu.

`<serverfile>`	Specifies the name of the server file to transfer to the PC.
`to <clientfile>`	Specifies the name of the PC file to be created.
	For most **REGET**operations, you can omit this option. When this option is omitted, the client file receives the same name as the server file.
	If the interrupted file transfer specified that the downloaded file be given a new name on the PC, be sure to use that name as the `<clientfile>` specification. This ensures that the Client can find the partial local file and successfully resume the transfer.
	The TO keyword is optional.

RENAME

Syntax: `rename <server filename> <new filename>`

FTP Command Index (page 848) SFTP Command Index (page 883)

The **RENAME**command changes the name of a server file to the new name specified. On some servers, you can use **RENAME**to specify both a new name and a new location for the file. In this case, the file is moved to the new location and given the new name specified.

`<server filename>`	Specifies the name of the server file you want to rename. The specification can include the name of the server folder where the file is located. Use quotation marks if the file or path includes spaces. For example: `"/Maps/North America"`.
`<new filename>`	Specifies the name you want to give the file. Use quotation marks if the file or path includes spaces. For example:
	`"D:\To do\Work assignments"`.
	On some servers, if you omit the path to the file you are renaming, the file is moved to the current server folder and given the new name. If you want to use **RENAME** to move a file, specify a new location and file name.

Example

In the current folder on the server, this command renames the file "Map of Canada" to "Canada":

`RENAME "Map of Canada" Canada`

From the "Maps" folder on the server , this command renames a file in the folder "Europe", changing the name from "England" to "Great Britain".

`RENAME /Maps/Europe/England "/Maps/Europe/Great Britain"`

SET

Syntax: `set <set parameter> <value>`

Use the **SET**command to configure Reflection. See the SET Parameters (page 869) for a list of available options.

Examples

These commands initialize various file transfer parameters:

```
SET TABS-TO-SPACES NO
SET TRANSFER-DISPOSITION Overwrite
SET TRANSFER-METHOD Ascii
SET TRANSLATE-FILES NO
```

Related Topics

- "SET Parameter Reference" on page 869
- "SET Parameters and Equivalent Interface Settings" on page 877
- "Site-Specific File Transfer SET Parameters" on page 879

SET Parameter Reference

The following parameters are for use with the "SET" on page 894 command. Settings are site-specific unless otherwise stated.

SET Parameter	Values	Description
ABORT-ON-ERROR	YES | NO (Default: YES)	Specifies whether execution of a script stops whenever an error occurs in response to a command. See "ABORT-ON-ERROR Script Sample" on page 881 for an example.
ACCOUNT	<string> (there is no default value)	Specifies the name of the account to log into on an FTP server. This setting does not apply to SFTP connections.
ANONYMOUS	YES | NO (Default: NO)	When set to YES, the client performs an anonymous login, using the user name "anonymous."
ASCII-CLIENT-TYPE	<value> (Default: WINDOWS)	When TRANSLATE-FILES and/or TRANSLATE-DIRECTORY-LISTING is YES, specifies the character set to use on the client PC during ASCII file transfers. Possible values are: PC-ENGLISH (IBM PC extended characters), PC-SLAVIC (DOS 852 code page), WINDOWS, WINDOWS-ANSI, WINDOWS-LATIN-2, WINDOWS-CYRILLIC, WINDOWS-GREEK, YUASCII. This setting does not apply to SFTP connections.

SET Parameter	Values	Description
ASCII-SERVER-TYPE	<value> (Default: DEC Supplemental)	When TRANSLATE-FILES and/or TRANSLATE-DIRECTORY-LISTING is YES, specifies the FTP server character set to use during ASCII file transfers. Possible values (page 880). This setting does not apply to SFTP connections.
AUTO-SERVER- UPDATE	YES | NO (Default: YES)	This global parameter specifies whether the server directory listing shown in the right pane is updated when you perform any operation that adds or deletes files or directories on the server.
CLIENT-HOME- DIRECTORY	<string>	Specifies the path to a home (default) directory for the local PC. If this setting is not set, the global **Default local home directory** setting is used.
CONFIRM-DELETE	YES | NO (Default: YES)	This global parameter specifies whether the client should prompt for confirmation before deleting a file.
CREATE-SERVER- UPPER	YES | NO (Default: NO)	Specifies whether all files transferred to the server are given uppercase file names.
CREATE-8.3-FILENAMES	YES | NO (Default: NO)	Specifies whether files transferred to the client use the 8.3 file naming convention.
CTRL-Z-EOF	YES | NO (Default: NO)	Applies to ASCII file transfers to a server. When this parameter is set to YES, file transfer uses Ctrl-Z as the end-of-file marker and strips it from the file being sent. When set to NO; the character count in the file directory entry is used to determine the file length. This setting does not apply to SFTP connections.
DELETE- TRAILING-SPACES	YES | NO (Default: NO)	Specifies whether to delete trailing spaces during ASCII file transfers from the server. This setting does not apply to SFTP connections.
EMAIL-ADDRESS	<string> (there is no default value)	This global parameter specifies your Internet email address. When opening a connection, most anonymous FTP sites ask you to supply your email address, which is used as the password for your guest login. Anonymous connections are not available for SFTP sessions.
FULL-TO-HALF-FROM- SERVER	YES | NO (Default: NO)	Applies to ASCII file transfers from the server. If you want messages and files with DEC Kanji or JIS Kanji characters to be converted from full- to half-width Katakana when received from the server, set this value to YES. The ASCII-SERVER-TYPE parameter determines which Kanji character set is used during the conversion.

SET Parameter	Values	Description
HALF-TO-FULL- TO-SERVER	YES | NO (Default: NO)	Applies to ASCII file transfers to the server. If you want files with DEC Kanji or JIS Kanji characters to be converted from half- to full-width Katakana when sent to the server, set this value to YES. The ASCII-SERVER-TYPE parameter determines which Kanji character set is used during the conversion.
ISO7-TO-ROMAN8	YES | NO (Default: NO	Applies to ASCII file transfers from the server when TRANSLATE-FILES is YES. If you want files with ISO-7 characters to be converted to files with Roman 8 characters when received on the PC, set this value to YES. The NATIONAL-REPLACEMENT-SET parameter determines the character conversion.
KANJI-AUTO-DETECT	YES | NO (Default: NO)	Specifies whether the client should automatically try to detect the type of Kanji character set (JIS, EUC, or DEC) used in any ASCII file and or message received from the server and then use the detected Kanji set for character translations.
MCS-TO-NRC	YES | NO (Default: NO)	Determines character set translation during ASCII file transfers to the server when TRANSLATE-FILES is YES. When set to YES, characters are translated from the DEC Multinational character set to the current national replacement character set. The NATIONAL-REPLACEMENT-SET value determines the character conversion.
NATIONAL-REPLACEMENT- SET	<value> (Default: USASCII)	Relevant when TRANSLATE-FILES and/or TRANSLATE-DIRECTORY-LISTING is YES. If necessary, set this parameter to match the set used by your host. Character translations occur between the client and the server when a PC file is sent to the server, and when characters sent from the server are written to local files, to the screen, or both. Possible values (page 881). This setting does not apply to SFTP connections.
NRC-TO-MCS	YES | NO (Default: NO)	Determines character set translation during ASCII file transfers from the FTP server to the PC when TRANSLATE-FILES and/or TRANSLATE-DIRECTORY-LISTING is YES. When set to YES, characters are translated from the current national replacement character set to the DEC Multinational Character set. The NATIONAL-REPLACEMENT-SET value determines the character conversion. This setting does not apply to SFTP connections.

SET Parameter	Values	Description
PASSIVE	YES | NO (Default: YES)	Specifies whether the client will send a PASV command to communicate with the server in passive mode (sometimes called PASV mode). Setting PASSIVE to YES causes the FTP Client to initiate a separate data connection for directory listings and file transfers. Passive mode is required for connections through some firewalls. This setting does not apply to SFTP connections.
PASSTHROUGH-AUTHENTICATION	YES | NO (Default: NO)	You must be connected to a site to change this global passthrough server property. Set PASSTHROUGH-AUTHENTICATION to YES if your passthrough server requires you to provide a user name and password to log into the passthrough server. This setting is ignored if USE-PASSTHROUGH-SERVER is set to NO or if PASSTHROUGH-SERVER-STYLE is set to SITE-SERVERNAME.
PASSTHROUGH-PASSWORD	<string> (there is no default value)	You must be connected to a site to change this global passthrough server property. This setting specifies your password on the passthrough server on your local network. For case-sensitive servers, you must use the appropriate case when you enter this value.
PASSTHROUGH- SERVER-STYLE	<value> (Default: SITE-SERVERNAME)	You must be connected to a site to change this global passthrough server property. The FTP Client sends different commands to log into the passthrough server and connect to an FTP server, based on the style of server (page 779) you specify. .
PASSTHROUGH-SERVERNAME	<string> (there is no default value)	You must be connected to a site to change this global passthrough server property. This setting specifies the name of the passthrough server on the local network that you use to log on to an FTP server.
PASSTHROUGH-USERNAME	<string> (there is no default value)	You must be connected to a site to change this global passthrough server property. Use this setting to specify a valid user name registered on the passthrough server for your local network. For case-sensitive servers, you must use the appropriate case when entering the PASSTHROUGH-USERNAME value.
PASSWORD	<string> (there is no default value)	Specifies your password on the current FTP server.
PORT-NUMBER	0 - 65535 (Default: 0)	Specifies a non-standard TCP service port number or socket for FTP. The default value 0 (zero) directs the FTP Client to use the standard service port for FTP, which is 21. This setting does not apply to SFTP connections.

SET Parameter	Values	Description
PRESERVE-FILE- DATE	YES | NO (Default: NO)	Specifies whether files that are downloaded from the server should retain the original date stamps associated with the files. If you want files transferred from the server to be date stamped with the time and date when they were transferred, set this parameter to NO.
PROXY-SERVER	<value>	This is a read-only parameter that indicates whether the FTP Client connects to this site using a passthrough server or SOCKS proxy server. The possible values are PROXY SERVER and SOCKS PROXY.
QUIET-STATUS	YES | NO (Default: NO)	This global parameter suppresses dialog box display, including Connection progress, Transfer progress, and Error notification.
RESUME-PARTIAL-TRANSFERS	ALWAYS | NEVER | ASKUSER (Default: ASKUSER)	This session-specific parameter is relevant for downloading files from the server in BINARY format. When you GET a server file, the FTP Client detects whether a prior incomplete download operation occurred for that file. This parameter allows you to control whether the Client prompts for input when it detects that a prior partial download occurred. Auto resume compares the size of the source file to the size of the incomplete target file to determine at what point in the source file it should resume the transfer. Using the binary method ensures that the file created on the local machine matches the size of the source file.
ROMAN8-TO-ISO7	YES | NO (Default: NO)	Applies to ASCII file transfers to the server when TRANSLATE-FILES is YES. If you want files with Roman 8 characters to be converted to files with ISO-7 characters when transferred to the server, set this value to YES. This setting does not apply to SFTP connections.
SAVE-PASSWORD	YES | NO (Default: NO)	Specifies whether the site password is saved.
SAVE-PASSTHROUGH-PASSWORD	YES | NO (Default: NO)	You must be connected to a site to change this global passthrough server property. When set to NO, the passthrough password is not saved.
SERVER-HOME-DIRECTORY	<string>	Specifies the path to a home (default) directory for the FTP or SFTP site to which you are currently connected. When a connection to the FTP or SFTP site is opened, the server working directory is set automatically to the specified home path. If no value is specified, the user home directory is used.

SET Parameter	Values	Description
SERVERNAME	<string> (there is no default value)	Specifies the name of the server that you want to log into. The server name is resolved via the Hosts file or a domain name server. If you have no domain name server on the local network and don't use a Hosts file, you must specify the full IP address. The value you specify is used the next time you open a connection during the current session.

SMART-ASCII- TYPES	<string>
	
	(DEFAULT: txt,bat,htm,html,ini)
		This global parameter specifies all the file extensions used to identify files that should be transferred using the ASCII transfer method when TRANSFER-METHOD is set to SMART. To specify a list of file extensions, separate each extension with a comma. For example:
		
		`SET SMART-ASCII-TYPES`
		`txt,bat,htm,html,ini`

SMART-BINARY- TYPES	<string> (DEFAULT: exe,gif,jpg,wav)	This global parameter specifies all the file extensions used to identify files that should be transferred using the Binary transfer method when TRANSFER-METHOD is set to SMART. To specify a list of file extensions, separate each extension with a comma. For example: `SET SMART-BINARY-TYPES exe,gif,jpg,wav`
SMART-TENEX- TYPES	<string> (there is no default value)	This global parameter specifies all the file extensions used to identify files that should be transferred using the Tenex (Local 8) transfer method when TRANSFER-METHOD is set to SMART. To specify a list of file extensions, separate each extension with a comma. For example: `SET SMART-TENEX-TYPES edd,gol,mmd,lad`
SMART-TYPE- DEFAULT	ASCII | BINARY | TENEX | ASK USER (Default: ASK USER	This global parameter specifies a default transfer method to use when TRANSFER-METHOD is set to SMART and the source file has an extension that has not been defined as either SMART-ASCII-TYPE, SMART-BINARY-TYPE, or SMART-TENEX-TYPE. During file transfers, if the source file uses an extension that has not been associated with a file transfer method, Smart File Transfer uses the transfer method specified for SMART-TYPE-DEFAULT.
SPACES-PER-TAB	1-20 (Default: 8)	Applies to ASCII file transfers. Specifies the number of consecutive spaces that are converted to a single tab character (for SPACES-TO-TABS) or the number of spaces that a single tab character is converted into (for TABS-TO-SPACES). This setting does not apply to SFTP connections.

SET Parameter	Values	Description
SPACES-TO- TABS	YES | NO (Default: NO)	Applies to ASCII file transfers from the host. When receiving ASCII files, you can replace consecutive spaces with tabs by setting this parameter to YES. The number of spaces that are converted to a single tab is controlled by the SPACES-PER-TAB parameter. This setting does not apply to SFTP connections.
TABS-TO- SPACES	YES | NO (Default: YES)	When set to YES, tab characters in local files are converted to space characters in server files during ASCII transfers to the server. The FTP Client replaces each tab character with the number of spaces necessary to fill out to the next tab stop, as specified by the SPACES-PER-TAB parameter. This setting does not apply to SFTP connections.
TIME-LOGGED-IN	(Read-only)	This is a read-only parameter that indicates the time when you logged into the server. The current time format specified in the International dialog box in the Windows Control Panel determines how time data displays.
TIME-SINCE- LOGIN	(Read-only)	This is a read-only parameter that indicates how long you have been logged into the server. The current time format specified in the International dialog box in the Windows Control Panel determines how time data displays.
TIMEOUT-CONNECT	0 - 65535 (Default: 120)	Specifies how long (in seconds) the client should continue trying to establish a server connection before it gives up. Setting this parameter to 0 (zero) prevents the FTP Client from ever timing out on a connection attempt. This setting does not apply to SFTP connections.
TIMEOUT- SESSION	0 - 65535 (Default: 120)	Specifies the maximum number of seconds to wait for data packets being transferred to or from the host. If nothing is received within the period specified, a timeout error displays and the transfer is aborted. Setting this parameter to 0 (zero) prevents the FTP Client from ever timing out when waiting for a response. This setting does not apply to SFTP connections.
TRANSFER-8.3- CASE	LOWER | UPPER | PRESERVE (Default: LOWER)	Specifies how case is handled in the names of files sent to the host, when the source file name conforms to the DOS 8.3 file naming convention. This setting is ignored when CREATE-SERVER-UPPER is set to yes.

SET Parameter	Values	Description
TRANSFER- DISPOSITION	<value> (Default: OVERWRITE)	This global parameter specifies a file transfer mode that tells the client what to do if the client or server file being transferred already exists at the destination. The possible values are APPEND, PROMPT, CANCEL, OVERWRITE, SKIP, UPDATE, UNIQUE. UPDATE directs the client to overwrite the destination file only if the file being transferred is newer than the destination file. UNIQUE directs the client to create a new unique name.
TRANSFER- ELAPSED-TIME	(Read-only)	This is a read-only parameter that indicates how long the last completed file transfer took to complete. The current time format specified in the International dialog box in the Windows Control Panel determines how time data displays.
TRANSFER-METHOD	<value> (Default: SMART)	This global parameter specifies the file transfer method for the client. The possible values are ASCII, BINARY, TENEX, SMART.
TRANSFER- SPEED	(Read-only)	This is a read-only parameter that indicates the speed of the last completed file transfer. This value represents the number of kilobytes transferred per second.
TRANSLATE- DIRECTORY-LISTING	YES | NO (Default: NO)	Specifies whether to enable translation when characters sent from the server are written to the screen. Use this setting to translate file names in server directory listings that display in the FTP Client user interface. Setting this parameter to YES enables the following SET parameters: SET ASCII-CLIENT-TYPE, SET ASCII-SERVER-TYPE, SET NATIONAL-REPLACEMENT, ISO7-TO-ROMAN8, and SET NRC-TO-MCS. This setting does not apply to SFTP connections.
TRANSLATE- FILES	YES | NO (Default: NO)	Specifies whether to enable translation of ASCII files. When set to YES, character translations occur between the client and the server when a PC file is sent to the server, and when characters sent from the server are written to a client file. Setting this parameter to YES enables the following SET parameters: SET ASCII-CLIENT-TYPE, SET ASCII-SERVER-TYPE, SET NATIONAL-REPLACEMENT, SET ISO7-TO-ROMAN8, SET ROMAN8-TO-ISO7, SET NRC-TO-MCS, and SET MCS-TO-NRC. This setting does not apply to SFTP connections.

SET Parameter	Values	Description
USE-PASSTHROUGH-SERVER	YES | NO (Default: NO)	Specifies whether to connect through a passthrough server when opening connections to the current FTP site. When set to YES, the FTP Client uses the following global settings to make the connection to the passthrough server: PASSTHROUGH-SERVER-STYLE, PASSTHROUGH-SERVERNAME, PASSTHROUGH-USERNAME, PASSTHROUGH-PASSWORD, and PASSTHROUGH-AUTHENTICATION.
USE-SOCKS	YES | NO (Default: NO)	Specifies whether you want to use a SOCKS proxy server for connections made to the current site. When set to YES, the FTP Client uses a SOCKS proxy server.
USERNAME	<string> (there is no default value)	Specifies a valid user name registered on the current server. For case-sensitive servers, you must use the appropriate case when entering the USERNAME value.
WRITE-CTRLZ	YES | NO (Default: NO)	Applies to ASCII file transfers from the server. When set to YES, the FTP Client automatically adds an end-of-file marker (^Z) at the end of a received ASCII file.

SET Parameters and Equivalent Interface Settings

SET parameters are for use with the "SET" on page 894 command. This table lists equivalent settings in the FTP Client user interface.

SET Parameter	Equivalent Interface Setting
ABORT-ON-ERROR	No equivalent dialog box setting
ACCOUNT	**Account** box on **Connection** tab in **Site Properties** dialog box
ANONYMOUS	**Anonymous** option on **General**tab in **Site Properties**dialog box
ASCII-CLIENT-TYPE	**Client** character set in **Character Sets** dialog box
ASCII-SERVER-TYPE	**Server** character set in **Character Sets** dialog box
AUTO-SERVER- UPDATE	**Refresh directory automatically** check box on the Directories tab in the **Site Properties** dialog box
CLIENT-HOME- DIRECTORY	**Local Home folder** box on the **Directories**tab in the **Site Properties** dialog box
CONFIRM-DELETE	**Confirm file delete** check box on the **Preferences** tab in the **Options** dialog box
CREATE-SERVER- UPPER	**Set case of 8.3 file names** list box on the **Transfer** tab in the **Site Properties** dialog box
CREATE-8.3- FILENAMES	**Create Windows file names in 8.3 format** check box on the Transfer tab in the **Site Properties** dialog box
CTRL-Z-EOF	**Read Ctrl-Z as end of file** under **To server** in the Translation tab **Site Properties** dialog box

SET Parameter	Equivalent Interface Setting
DELETE-TRAILING- SPACES	**Delete trailing spaces** check box on the **Translation** tab in **Site Properties** dialog box
EMAIL-ADDRESS	**Anonymous password** box on the **General** tab in the **Options** dialog box
FULL-TO-HALF-FROM- SERVER	**Full- to half-width Katakana** check box in **Character Sets** dialog box
HALF-TO-FULL-TO- SERVER	**Half- to full-width Katakana** check box in **Character Sets** dialog box
ISO7-TO-ROMAN8	**Change ISO-7 to Roman-8** check box in **Character Sets** dialog box
KANJI-AUTO-DETECT	**Detect server Kanji type** check box in **Character Sets** dialog box
MCS-TO-NRC	**Change MCS to NRC** check box in **Character Sets** dialog box
NATIONAL-REPLACEMENT-SET	**ISO-7/NRC** set in **Character Sets** dialog box
NRC-TO-MCS	**Change NRC to MCS** check box in **Character Sets** dialog box
PASSIVE	**Use passive mode** check box on **Connection** tab in the **Site Properties** dialog box
PASSTHROUGH- AUTHENTICATION	**Use Firewall** check box on the **Firewall** tab in the **Security Properties** dialog box
PASSTHROUGH- SERVERNAME	**Server name** box on the **Firewall** tab in the **Security Properties** dialog box
PASSTHROUGH- USERNAME	**User name** box on the **Firewall** tab in the **Security Properties** dialog box
PASSWORD	**Password** box on **General** tab in the **Site Properties** dialog box
PORT-NUMBER	**TCP port** box on **Connection** tab in the **Site Properties** dialog box
PRESERVE-FILE- DATE	**Preserve server file date** check box on the Transfer tab in the **Site Properties** dialog box.
PROXY-SERVER	Read-only value based firewall and SOCKS configuration in the **Security Properties** dialog box.
QUIET-STATUS	**Hide progress window** check box on the Preferences tab in the **Options** dialog box
ROMAN8-TO-ISO7	**Change Roman-8 to ISO-7** check box in the **Character Sets** dialog box
SAVE-PASSWORD	**Save password** check box on the **General** tab in the **Site Properties** dialog box
SAVE-PASSTHROUGH- PASSWORD	**Save password** check box on the **Firewall** tab in the **Security Properties** dialog box
SERVER-HOME- DIRECTORY_SERVER_HOME_DIRECTORY	**Server Home directory** box on the **Directories** tab in the **Site Properties** dialog box
SERVERNAME_SERVERNAME	**FTP address** box on the **General** tab in the **Site Properties** dialog box
SMART-ASCII-TYPES	File transfer types on the **File Types** tab in the **Options** dialog box

SET Parameter	Equivalent Interface Setting
SMART-BINARY-TYPES	File transfer types on the **File Types** tab in the **Options**dialog box
SMART-TENEX-TYPES	File transfer types on the **File Types** tab in the **Options**dialog box
SMART-TYPE-DEFAULT	**Transfer method for undefined file types** group box on the **File Types** tab in the **Options**dialog box
SPACES-PER-TAB	**Spaces per tab** box on **Translation**tab in the **Site Properties** dialog box
SPACES-TO-TABS	**Change spaces to tabs** check box on **Translation**tab in the **Site Properties** dialog box
TABS-TO-SPACES	**Change tabs to spaces** check box on **Translation**tab in the **Site Properties** dialog box
TIME-LOGGED-IN	**Connected at** on the **Information**tab in the **Site Properties** dialog box
TIME-SINCE-LOGIN	**Connected for** on the **Information**tab in the **Site Properties** dialog box
TIMEOUT-CONNECT	**Connect** box on the **Connection**tab in the **Site Properties** dialog box
TIMEOUT-SESSION	**Session** box on the **Connection**tab in the **Site Properties** dialog box
TRANSFER-8.3-CASE	**Set case of 8.3 file names** box under **Upload to server options** on the **Transfer**tab in the **Site Properties** dialog box
TRANSFER- DISPOSITION	**If File Exists** command on the **Tools**menu
TRANSFER-ELAPSED- TIME	**Last transfer time** on the **Information**tab in the **Site Properties** dialog box
TRANSFER-METHOD	**Transfer Method** command on the **Tools**menu
TRANSFER-SPEED	**Last transfer rate** on the **Information**tab in the **Site Properties** dialog box
TRANSLATE-FILES	**Translate files** check box in **Character Sets** dialog box
USE-PASSTHROUGH- SERVER	Controlled by firewall configuration in the **Security Properties** dialog box.
USE-SOCKS	Controlled by SOCKS configuration in the **Security Properties** dialog box.
USERNAME	**User** box on **General**tab in the **Site Properties** dialog box
WRITE-CTRLZ	**Write Ctrl-Z at end of file** under **From server** on **Translation**tab in **Site Properties** dialog box

Site-Specific File Transfer SET Parameters

Advanced File Transfer SET Parameters

Transfer options when sending files to the server

- CREATE-SERVER-UPPER
- TRANSFER-8.3-CASE

Transfer options when receiving files from the server

- ◆ PRESERVE-FILE-DATE
- ◆ CREATE-8.3-FILENAMES

Character Translation SET Parameters for ASCII File Transfer

Character sets used for translations

- ◆ ASCII-CLIENT-TYPE
- ◆ ASCII-SERVER-TYPE
- ◆ NATIONAL-REPLACEMENT-SET

Translation options when sending files to the server

- ◆ MCS-TO-NRC
- ◆ ROMAN8-TO-ISO7

Translation options when receiving files from the server

- ◆ ISO7-TO-ROMAN8
- ◆ NRC-TO-MCS

ASCII-SERVER-TYPE SET Parameter Values

The ASCII-SERVER-TYPE **SET** parameter (page 869) `<value>` can be any of the following:

DEC-SUPPLEMENTAL	ISO-LATIN-2	BIG-5	DEC-Hebrew
ISO-LATIN-1	ISO-LATIN-5	CCDC	7-Bit-Hebrew
PC-ENGLISH	ISO-LATIN-6	GB-Chinese	DEC-Cyrillic
PC-MULTILINGUAL	ISO-LATIN-7	KS-5601-Korean	HP-Turkish
HP-ROMAN-8	ISO-LATIN-8	HP-Greek	DEC-Turkish
PC-SLAVIC	ISO-LATIN-9	DEC-Greek	PC-Spanish
PC-CYRILLIC-855	SHIFT-JIS	PC-Greek	PC-Turkish
PC-MODERN-TURKISH	JIS-X0208-1990	YUASCII	SBIG-5
PC-PORTUGUESE	JIS-X0208-1983	PC-Cyrillic	THAI-988-TISO
PC-ICELANDIC	JIS-C6226-1978	JIS-Katakana	THAI-TISO
PC-CANADIAN-FRENCH	DEC-1983-KANJI	NEC-N88	THAI-KU
PC-ARABIC	DEC-1978-KANJI	PC-Hebrew	THAI-PRIME
PC-NORDIC	EUC	HP-Hebrew	HP-Hebrew
PC-MODERN-GREEK	PC-MODERN-GREEK		

NATIONAL-REPLACEMENT-SET Parameter Values

The NATIONAL-REPLACEMENT-SET **SET** parameter (page 869) `<value>` can be any of the following::

USASCII	GERMAN
DANISH	SWISS-GERMAN
DUTCH	ITALIAN
CANADIAN-ENGLISH	SPANISH-LATIN
FINNISH	NORWEGIAN
FLEMISH	PORTUGUESE
FRENCH	SPANISH-EUROPEAN
CANADIAN-FRENCH	SWEDISH
SWISS-FRENCH	BRITISH

ABORT-ON-ERROR Script Sample

This sample code sets **ABORT-ON-ERROR** (page 869) to NO before using "MGET" on page 860 and back to YES before using "MDEL" on page 860 or "PUT" on page 865.

```
SET ABORT-ON-ERROR NO
CD /home/user1/reports
CONTINUE ON
MGET june*.rpt
CD /home/user2/reports
MGET june*.rpt
SET ABORT-ON-ERROR YES
MDEL june*.rpt
CD /home/user1/reports
MDEL june*.rpt
SET ABORT-ON-ERROR NO
CD /home/yearly
CONTINUE
MGET ye20*.rpt,ye20*.txt
SET ABORT-ON-ERROR YES
CD /tmp
PUT ye2000.txt
PUT ye2000.rpt ye2000.txt APPEND
```

SITE

Syntax: `site <argument>`

FTP Command Index (page 848)

The **SITE** command allows you to send a recognized **SITE** command to the server.

To find out what **SITE** commands are understood by the current FTP server, try entering this command at the FTP command line:

```
QUOTE help site
```

If the server supports the **QUOTE** command, it may respond with a list the **SITE** commands that are understood by the server. The server response displays in the command window.

<argument>   Specifies any **SITE** command that the FTP server understands.

Examples

The following command requests the idle timeout setting for the server:

SITE idle

The server response shows in the command window. For example:

200 Current IDLE time limit is 900 seconds; max 7200

This command sets the IDLE timeout to 1800 seconds:

SITE idle 1800

SMART

Syntax: smart

FTP Command Index (page 848)   SFTP Command Index (page 883)

The **SMART**command changes the current FTP file transfer method to Smart.

Use the Smart transfer method if you want the FTP Client to automatically determine what transfer method to use (ASCII, Binary, or Tenex) based on the type of file that is being transferred. The FTP Client uses the source file extension to determine what type of file is being transferred. To set up for Smart File Transfer, use settings on the **File Types** tab in the **Options** dialog box.

SYSTEM

Syntax: system

FTP Command Index (page 848)

The **SYSTEM**command displays information about the type of operating system used by the current FTP server. The information displays in the FTP command window.

For example, if you entered **SYSTEM** at the FTP command line, the display might look like this:

215 UNIX Type: L8

TENEX

Syntax: tenex

FTP Command Index (page 848)   SFTP Command Index (page 883)

The **TENEX**command changes the current file transfer method to "local 8." Use this transfer method if you're moving files to or from a server that uses a non-8-bit byte (such as the DECsystem-20).

TYPE

Syntax: `type <serverfile>`

The **TYPE**command displays the contents of a server file in the FTP command window.

`<serverfile>` Specifies the location and name of the server file. This specification cannot contain wildcards.

Example

The following command displays in the command window the file hardware.txt, which is located in the /Users/boris folder on the FTP server:

`TYPE /Users/boris/hardware.txt`

VERIFY

Syntax: `verify [commands] [<set parameter>] [changed]`

The **VERIFY**command displays information about the values of one or more **SET parameters (page 869)**. With no parameters, **VERIFY** displays the current value of all Reflection **SET**parameters.

`<set parameter>` Displays the value of a particular **SET**parameter.

Examples

This command displays the current national replacement set setting:

`VERIFY NATIONAL-REPLACEMENT-SET`

This command creates a complete list of current SET parameter values:

`VERIFY`

SFTP commands

In this Section

ASCII

Syntax: `ascii`

The **ASCII** command changes the current file transfer method to ASCII. Use this transfer method to move ASCII text files between the server and your PC.

BINARY

Syntax: `binary`

The **BINARY** command changes the current file transfer method to binary (image). Use this transfer method to transfer binary files, such as .EXE files and compressed files, between two PCs (via a server), or between two servers (via a PC).

BYE

Syntax: `bye`

The **BYE** command closes the connection to the server.

This command is available for SFTP connections only.

CD

Syntax: `cd <server directory>`

The **CD** command changes the working directory on the FTP server.

`<server directory>`   Specifies a directory on the server.

Examples

This command changes to the directory "Asian Artists" on a UNIX system:

`CD Asian Artists`

This command changes directories on a VAX/VMS system:

`CD SYS$USERS:[ARNOLD.DOCS]`

CHMOD

Syntax: `chmod <numeric permission mask> <server file or directory>`

The **CHMOD** command changes the permissions associated with a file or directory.

`<numeric permission mask>`	Specifies a three digit numeral that is a valid value for the UNIX chmod command. Valid values have digits from 0 to 7.
	Tip: To determine what mask to use to set permissions, right click on a server file and select properties. The properties dialog box displays the three digit mask and the permissions associated with it. If you change the permissions, the mask value is updated automatically.
`<server file or directory>`	Specifies a file or directory on the FTP server. Follow the server's syntax for specifying file and directory names.

Example

This command sets attributes to `-rw-r--r--` for the specified file.

`chmod 644 myfile.htm`

EXIT

Syntax: `exit`

The **EXIT**command closes the connection to the server.

GET

Syntax: `get <serverfile> [to] [<clientfile>] [append | askuser | cancel | overwrite | skip | unique]`

The **GET**command transfers a file from the server to the PC. Wildcards are not supported with the **GET**command—they are treated as ordinary characters and are assumed to be part of the file name. To transfer multiple files, use "MGET" on page 860.

Before using the **GET**command, if necessary, use the "ASCII" on page 884, "BINARY" on page 851, "TENEX" on page 895, or "SMART" on page 894 command to override the default file transfer method setting specified on the **Tools** menu.

A variety of site-specific **SET**parameters can affect the transfer operation. Click here (page 879) for more information.

`<serverfile>`	Specifies the name of the server file.
`to <clientfile>`	Specifies the name of the PC file to be created. If this option is omitted, the client file receives the same name as the server file. The TO keyword is optional.
`append	askuser	cancel	overwrite	skip	unique`	Specifies what to do if the destination file already exists. If this option is omitted, the active **TRANSFER-DISPOSITION** (page 869) setting is the default.

Examples

The following example transfers the server file MEMO.DOC from the server to the PC, giving the PC file the same name:

```
GET MEMO.DOC
```

This example transfers the VAX/VMS FTP server file MORTGAGE.PAPERS to the PC, giving the PC file the name MORTGAGE.TXT:

```
GET MORTGAGE.PAPERS MORTGAGE.TXT
```

LCD

Syntax: `lcd [<pc drive/folder> | ..]`

The **LCD** command opens another folder on the PC.

If no `<folder>` is specified, **LCD** displays the path for the current PC folder.

To change folders, type the folder at the FTP command line, for example, type `LCD F:\Documents`and press Return.

`<pc drive/folder>`	Specifies the drive (if other than the current drive) and folder to change to.
`..`	Specifies that you want to change to the parent folder.

Example

This command changes your current folder to the China folder within the Asian Travel folder on drive D:

`LCD d:\Asian Travel\China`

LLS

Syntax: `lls [<pc filespec>]`

The **LLS** command displays a listing of PC files matching the given filespec.

This command is available for SFTP connections only. The FTP equivalent is **LDIR**.

`<pc filespec>`	Specifies a folder, a file, or a group of files on the PC. If this option is not used, the contents of the current PC folder are displayed.

Example

This command displays a listing of files in the current PC folder that have a .Doc extension:

`LLS *.Doc`

LMKDIR

Syntax: `lmkdir <pc directory>`

The **LMKDIR** command creates a folder on the PC.

This command is available for SFTP connections only. The FTP equivalent is **LMD**.

`<pc folder>`	Specifies the drive where you want to create the folder (if other than the current drive) and the folder name.

Example

This command creates the folder Music on the current PC drive:

`LMKDIR \Music`

LPWD

Syntax: `lpwd [<pc drive/folder> | ..]`

The **LPWD** command opens another folder on the PC.

If no `<folder>` is specified, **LPWD** displays the path for the current PC folder.

To change folders, type the folder at the FTP command line, for example, type `LPWD F:\Documents` and press Return.

This command is available for SFTP connections only. The FTP equivalent is **LCD**.

`<pc drive/folder>`	Specifies the drive (if other than the current drive) and folder to change to.
`..`	Specifies that you want to change to the parent folder.

Example

This command changes your current folder to the China folder within the Asian Travel folder on drive D:

`LPWD d:\Asian Travel\China`

LS

Syntax: `ls [<server filespec>]`

The **LS** command displays a simple listing of server files matching the given filespec. (Compare this to the "DIR" on page 854 command, which displays a more detailed listing.)

`<server filespec>`	Specifies a folder, file, or group of files on the server. If this option is not used, the contents of the current server folder are displayed.

Example

In this example, the names of all files in the current folder on a UNIX FTP server are listed:

`LS *.*`

MGET

Syntax: `mget <server filespec> [to] [<pc filespec>] [append | askuser | cancel | overwrite | skip | unique]`

The **MGET** command transfers one or more files matching the given filespec from the FTP server to the PC. You can use wildcards to transfer multiple files. Most servers support wildcards in the `<serverspec>`. However, if your server doesn't support wildcards in an command, using **MGET** with a wildcard specification may result in a transfer of all files in the current directory.

NOTE: The Reflection client supports **MGET** in SFTP sessions, however you should test transfers that use wildcard characters because the SFTP server may not interpret wildcard specifications correctly.

Before using the **MGET** command, if necessary, use the , , , or command to override the default file transfer method setting specified on the Tools menu.

A variety of site-specific **SET** parameters can affect the transfer operation. for more information.

`<server filespec>`	Specifies one server file or (using server wildcards) multiple server files to transfer to the PC. If a `<server filespec>`is given with no other options, the PC files are given the same names as the server files.
`to <pc filespec>`	Specifies a PC folder to receive the files, or the name of the PC file to create. The TO keyword is optional. If this option is omitted, server files are transferred to the current folder.
	If `<server filespec>` specifies more than one file, the `<pc filespec>` should typically be a directory path. To consolidate a series of server files in one PC file, you can specify a file name for the `<pc filespec>` and use the APPEND option.
	Use quotation marks if the file or path includes spaces. For example:
	`MGET *.* "C:\My documents\*.*"`
`append	askuser	cancel	overwrite	skip	unique`	Specifies what to do if the destination file already exists. If this option is omitted, the active **TRANSFER-DISPOSITION** (page 869) setting is the default.

Examples

This example transfers all files with a .Doc extension from the FTP server to the PC, placing the files in the current PC directory:

`MGET *.Doc`

This example adds the letter A to the transferred files. For example, test.txt becomes Atest.txt.

`MGET *.* A*.*`

See for an additional example.

MKDIR

Syntax: `mkdir <server folder>`

The **MKDIR** command creates a folder on the server.

This command is available for SFTP connections only. The FTP equivalent is **MD**.

`<server folder>`   Specifies the name and location of the new folder.

Example

This command creates the folder Films within the current folder on the current FTP UNIX server drive:

```
MKDIR Films
```

MPUT

Syntax: `mput <pc filespec> [to] [<server filespec>] [append | askuser | cancel | overwrite | skip | unique]`

FTP Command Index (page 848)   SFTP Command Index (page 883)

The **MPUT** command transfers one or more files matching the given filespec from the PC to the FTP server. You can use wildcards to transfer multiple files.

NOTE: The Reflection client supports **MPUT** in SFTP sessions, however you should test transfers that use wildcard characters because the SFTP server may not interpret wildcard specifications correctly.

Before using the **MPUT** command, if necessary, use the "ASCII" on page 884, "BINARY" on page 851, "TENEX" on page 895, or "SMART" on page 894 command to override the default file transfer method setting specified on the **Tools** menu.

A variety of site-specific **SET** parameters can affect the transfer operation. Click here (page 879) for more information.

`<pc filespec>`	Specifies one PC file or (using wildcards) multiple PC files to transfer to the server. The files are placed in the current server directory and are given the same names as the PC files.
	PC wildcard characters (the ? and * characters) can be used to send multiple files to the server. For example, to send all files in the current directory with the file extension `.Txt`, use the command `MPUT *.Txt`.
	Use quotation marks if the file or path includes spaces. For example:
	`MPUT "C:\My documents\*.*"`
`to <server filespec>`	Specifies a server file or (using server wildcards) multiple server files to receive the PC files. If files of this name don't exist, they are created by the transfer. If no value for <server filespec> is given, server files are given the same name as the PC files.
	The TO keyword is optional.
`append | askuser | cancel | overwrite | skip | unique`	Specifies what to do if the destination file already exists. If this option is omitted, the active **TRANSFER-DISPOSITION** (page 869) setting is the default.

Examples

The following example transfers files in the Meeting Notes folder within the current folder on the PC that have a .Doc extension , placing the files in the current server folder. Source PC files that have the same name as files in the destination server folder are not transferred.

```
MPUT "Meeting Notes\*.Doc" skip
```

The following example adds the letter "A" to the front of files transferred to the server. For example Sample.htm becomes ASample.htm.

```
MPUT *.htm A*.htm
```

The final example removes file extensions from PC files copied to the server:

```
MPUT *.*  *.
```

PROGRESS

Syntax: `progress`

SFTP Command Index (page 883)

Toggles the display of the progress meter.

This command is available for SFTP connections only.

PUT

Syntax: `put <clientfile> [to] [<serverfile>] [append | askuser | cancel | overwrite | skip | unique]`

FTP Command Index (page 848)   SFTP Command Index (page 883)

The **PUT**command transfers a file from the PC to the server.

Wildcards are not supported with the **PUT**command; to transfer multiple files using wildcards, use "MPUT" on page 862.

Before using the **PUT**command, if necessary, use the "ASCII" on page 884, "BINARY" on page 851, "TENEX" on page 895, or "SMART" on page 894 command to override the default file transfer method setting specified on the **Tools** menu.

A variety of site-specific **SET**parameters can affect the transfer operation. Click here (page 879) for more information.

`<clientfile>`	Specifies the name of the PC file. Use quotation marks if the file or path includes spaces.
`to <serverfile>`	Specifies the name of the server file to be created. If the server file name is omitted, the server file is given the same name as the PC file. The TO keyword is optional.
`append | askuser | cancel | overwrite | skip | unique`	Specifies what to do if the destination file already exists. If this option is omitted, the active **TRANSFER-DISPOSITION** (page 869) setting is the default.

Examples

The following example transfers the file Memo.doc from the PC to the server:

```
PUT Memo.doc
```

This example transfers the file HAPPY.ME from a PC to a VAX/VMS FTP server, giving the VMS file the name HAPPY.BIRTHDAY:

```
PUT HAPPY.ME TO HAPPY.BIRTHDAY
```

See "ABORT-ON-ERROR Script Sample" on page 881 for an additional example.

PWD

Syntax: `pwd`

FTP Command Index (page 848)   SFTP Command Index (page 883)

The **PWD**command shows the server folder that is currently open. The name and location of the folder display in the FTP command window.

QUIT

Syntax: `quit`

FTP Command Index (page 848)   SFTP Command Index (page 883)

The **QUIT**command closes the connection to the server.

NOTE: When you run a script from the Windows command line using the /RFS switch and the script ends in with a **QUIT** command, the FTP client shuts down automatically when the script is complete.

RENAME

Syntax: `rename <server filename> <new filename>`

FTP Command Index (page 848)   SFTP Command Index (page 883)

The **RENAME**command changes the name of a server file to the new name specified. On some servers, you can use **RENAME**to specify both a new name and a new location for the file. In this case, the file is moved to the new location and given the new name specified.

`<server filename>`	Specifies the name of the server file you want to rename. The specification can include the name of the server folder where the file is located. Use quotation marks if the file or path includes spaces. For example: `"/Maps/North America"`.
`<new filename>`	Specifies the name you want to give the file. Use quotation marks if the file or path includes spaces. For example: `"D:\To do\Work assignments"`. On some servers, if you omit the path to the file you are renaming, the file is moved to the current server folder and given the new name. If you want to use **RENAME** to move a file, specify a new location and file name.

Example

In the current folder on the server, this command renames the file "Map of Canada" to "Canada":

`RENAME "Map of Canada" Canada`

From the "Maps" folder on the server , this command renames a file in the folder "Europe", changing the name from "England" to "Great Britain".

`RENAME /Maps/Europe/England "/Maps/Europe/Great Britain"`

RM

Syntax: `rm <serverfile>`

The **RM**command deletes a file matching the given filespec on the SFTP server.

This command is available for SFTP connections only. The FTP equivalent is **DELETE**.

NOTE: If the **SET** parameter (page 869) CONFIRM-DELETE is set to YES, the user is prompted for confirmation before deleting.

`<serverfile>`	Specifies the name of a server file to delete. This can include a full directory path to the file. On some systems case is important when specifying directories and file names.

Example

This command deletes MEMO.DOC from the current server directory:

`RM MEMO.DOC`

RMDIR

Syntax: `rmdir <server folder>`

The **RMDIR** command deletes an empty folder on the server.

This command is available for SFTP connections only.

NOTE: If the **SET** parameter (page 869) CONFIRM-DELETE is set to YES, the user is prompted for confirmation before deleting.

`<server folder>`	Specifies the location and name of the folder you want to delete. The `<server folder>` specification must follow the conventions of the server operating system. Before you can delete a folder, you must delete the files and folders within it.

Example

This command deletes the folder Articles from the current server folder:

```
RMDIR Articles
```

SET

Syntax: `set <set parameter> <value>`

Use the **SET** command to configure Reflection. See the SET Parameters (page 869) for a list of available options.

Examples

These commands initialize various file transfer parameters:

```
SET TABS-TO-SPACES NO
SET TRANSFER-DISPOSITION Overwrite
SET TRANSFER-METHOD Ascii
SET TRANSLATE-FILES NO
```

Related Topics

- "SET Parameter Reference" on page 869
- "SET Parameters and Equivalent Interface Settings" on page 877
- "Site-Specific File Transfer SET Parameters" on page 879

SMART

Syntax: `smart`

The **SMART** command changes the current FTP file transfer method to Smart.

Use the Smart transfer method if you want the FTP Client to automatically determine what transfer method to use (ASCII, Binary, or Tenex) based on the type of file that is being transferred. The FTP Client uses the source file extension to determine what type of file is being transferred. To set up for Smart File Transfer, use settings on the **File Types** tab in the **Options** dialog box.

TENEX

Syntax: `tenex`

The **TENEX**command changes the current file transfer method to "local 8." Use this transfer method if you're moving files to or from a server that uses a non-8-bit byte (such as the DECsystem-20).

Glossary of Terms

Reflection Workspace menu. The Workspace menu contains layout options, application and document settings, and a list of recent documents. It is accessed by clicking the Reflection button ⬢ (when using the Office 2007 look and feel) or the **File**menu (when using the Office 2010 look and feel).

APVUFILE. A file transfer protocol used for transfers to and from double-byte enabled IBM 3270 hosts. Configure APVUFILE transfers from the **Mainframe** tab of the **File Transfer Settings** dialog box.

authentication. The process of reliably determining the identity of a communicating party. Identity can be proven by something you know (such as a password), something you have (such as a private key or token), or something intrinsic about you (such as a fingerprint).

Auto Expand. Use the Auto Expand feature to add acronyms or shortcuts for long words, phrases, or complex repeat commands. The shortcut, when typed and followed by the Spacebar, automatically expands to the full word or phrase.

CA (Certificate Authority). A server, in a trusted organization, which issues digital certificates. The CA manages the issuance of new certificates and revokes certificates that are no longer valid for authentication. A CA may also delegate certificate issuance authority to one or more intermediate CAs creating a chain of trust. The highest level CA certificate is referred to as the trusted root.

cipher. A cipher is an encryption algorithm. The cipher you select determines which mathematical algorithm is used to obscure the data being sent after a successful Secure Shell connection has been established.

credentials cache. The location of stored credentials. Credentials consist of session keys, TGTs, and service tickets issued to a client by the KDC. The client uses its credentials to authenticate itself when it requests a service.

CRL (Certificate Revocation List). A digitally signed list of certificates that have been revoked by the Certification Authority. Certificates identified in a CRL are no longer valid.

digital certificate. An integral part of a PKI (Public Key Infrastructure). Digital certificates (also called X.509 certificates) are issued by a certificate authority (CA), which ensures the validity of the information in the certificate. Each certificate contains identifying information about the certificate owner, a copy of the certificate owner's public key (used for encrypting and decrypting messages and digital signatures), and a digital signature (generated by the CA based on the certificate contents). The digital signature is used by a recipient to verify that the certificate has not been tampered with and can be trusted.

digital signature. Used to confirm the authenticity and integrity of a transmitted message. Typically, the sender holds the private key of a public/private key pair and the recipient holds the public key. To create the signature, the sender computes a hash from the message, and then encrypts this value with its private key. The recipient decrypts the signature using the sender's public key, and independently computes the hash of the received message. If the decrypted and calculated values match, the recipient trusts that the sender holds the private key, and that the message has not been altered in transit.

encryption. Encryption is the process of scrambling data by use of a secret code or cipher so that it is unreadable except by authorized users. Encrypted data is far more secure than unencrypted data.

Express Logon Feature (ELF). Also referred to as *single sign-on (SSO),* express logon is an IBM mainframe feature that lets users log on and connect to the host without entering a user ID and password each time. Express Logon authenticates the user on the mainframe by using her SSL client certificate in lieu of entering a user ID and password.

hash. Also called a message digest, a hash or hash value is a fixed-length number generated from variable-length digital data. The hash is substantially smaller than the original data, and is generated by a formula in such a way that it is statistically unlikely that some other data will produce the same hash value.

hosts file. A list that maps recognizable host names to Internet addresses, similar to a domain name system. You can use a hosts file whether there is a domain name server on your network.

Hotspots. Hotspots are specific areas or text that are associated with host functions, macros, or commands. When enabled, hotspots appear in the terminal area of a display session.

KDC (Key Distribution Center). The security server that maintains the database of principal information, uses the information in the database to authenticate users, and controls access to kerberized services in a realm.

Keyboard Map. A keyboard map is a configuration file that allows you to use your PC keyboard as a host terminal keyboard. keyboard maps also include definitions for keyboard shortcuts.

Layout. A layout is a settings file that you can create to restore your workspace and all open documents. It also restores the workspace position and tab properties of open documents.

LDAP (Lightweight Directory Access Protocol). A standard protocol that can be used to store information in a central location and distribute that information to users.

OCSP (Online Certificate Status Protocol). A protocol (using the HTTP transport) that can be used as an alternative to CRL checking to confirm whether a certificate is valid. An OCSP responder responds to certificate status requests with one of three digitally signed responses: "good", "revoked", and "unknown". Using OCSP removes the need for servers and/or clients to retrieve and sort through large CRLs.

Office Tools. The Office Tools feature allows you to integrate host data with Microsoft Office applications, if those applications are installed on your computer. You can create Word documents and PowerPoint presentations, send e-mail, schedule appointments, add notes and tasks, and create new contacts.

passphrase. A passphrase is similar to a password, except it can be a phrase with a series of words, punctuation, numbers, white space, or any string of characters. Passphrases improve security by limiting access to secure objects, such as private keys and/or a key agent.

PCI DSS. PCI DSS (Payment Card Industry Data Security Standard) is a worldwide standard comprising technology requirements and process requirements designed to prevent fraud and is published by PCI Security Standards Council, LLC. All companies who handle credit cards are likely to be subject to this standard.

PKCS. PKCS (Public Key Cryptography Standards) is a set of standards devised and published by RSA laboratories that enable compatibility among public key cryptography implementations. Different PKCS standards identify specifications for particular cryptographic uses, for example:

PKCS#7 can be used to sign and/or encrypt messages. It can also be used to store certificates and to disseminate certificates (for instance as a response to a PKCS#10 message).

PKCS#10 is a certification request syntax.

PKCS#11 is a programming interface used for cryptographic hardware tokens.

PKCS#12 defines the personal information exchange syntax used for storage and transportation of certificates and associated private keys. Files in this format typically use a *.pfx or *.p12 extension.

port forwarding. A way to redirect unsecured traffic through a secure SSH tunnel. Two types of port forwarding are available: local and remote. Local (also called outgoing) port forwarding sends outgoing data sent from a specified local port through the secure channel to a specified remote port. You can configure a client application to exchange data securely with a server by configuring the client to connect to the redirected port instead of directly to the computer running the associated server. Remote (also called incoming) port forwarding sends incoming data from a specified remote port through the secure channel to a specified local port.

principal profile. A collection of information that defines who you are (your principal and realm names) and which settings you want to use (requested ticket lifetime, how your credentials should be stored, and the name of your profile).

principals database. A database containing valid principals and passwords for a particular realm. Each realm has its own credentials database. This database is part of the KDC (Key Distribution Center).

Privacy Filters. This feature provides a way to filter out sensitive data (for example, Social Security or account numbers), and refrain from displaying it in productivity features, such as Office Tools integration, Screen History, Recent Typing, and Auto Complete, and to obscure data from the Print Screen and Cut/Copy/Paste commands.

product installation folder. The default is `\Program Files\Micro Focus\Reflection`.

Public Key Infrastructure (PKI). PKI is a framework of policies, services, and encryption software used for authentication and encryption of sensitive information. The PKI Framework depends on trusted third parties called certification authorities (CAs), which issue digital certificates.

public key/private key. Public keys and private keys are pairs of cryptographic keys that are used to encrypt or decrypt data. Data encrypted with the public key can only be decrypted with the private key; and data encrypted with the private key can only be decrypted with the public key.

Recent Typing. Using the Recent Typing gallery or task pane, you can quickly view and select from a list of recently typed items, and send the selected string to the active document. This eliminates the need to manually re-enter information, saving time, and reducing errors when entering commonly-typed commands or field data.

Reflection global ssh folder. Reflection stores global Secure Shell information in the Windows common application data folder. The default is `\ProgramData\Micro Focus\Reflection`.

Reflection ssh folder. Reflection stores Secure Shell information for individual users in the following location in the Windows personal documents folder. The default is `\Users\`*`username`*`\Documents\Micro Focus\Reflection\.ssh`.

Scratch Pad. Use the Scratch Pad to keep notes associated with a session. From the task pane you can print or save the Scratch Pad notes as .RTF or .TXT files.

Screen History. Screen History creates recordings of IBM 3270 and 5250 host screens as you navigate to them. VT screens can be recorded using manual capture. You can view and/or verify the information from those screens, and send multiple host screens to Microsoft Word, PowerPoint, and Outlook (Email Message and Note only), if they are installed on your computer.

secret key cryptography. In this form of cryptography, which is sometimes referred to as *symmetric cryptography*, data is encrypted and decrypted using the same key or shared secret quantity.

Secure Shell. A protocol for securely logging onto a remote computer and executing commands. It provides a secure alternative to Telnet, FTP, rlogin, or rsh. Secure Shell connections require both server and user authentication, and all communications pass between hosts over an encrypted communication channel. You can also use Secure Shell connections to forward X11 sessions or specified TCP/IP ports through the secure tunnel.

socket. The combination of a host name (IP address or DNS name) and a port number. This creates a unique identifier that a client application uses as an end point of communications.

SOCKS. SOCKS is a software protocol used in conjunction with a firewall host system to provide secure, controlled access to internal and external networks. When you request a network connection from a SOCKS-enabled application, the SOCKS Client software communicates with the SOCKS server software to determine if the connection is allowed. If it is, the connection is established. If it is not, the SOCKS server rejects the connection request.

SSL/TLS. The Secure Sockets Layer protocol (SSL) and its compatible successor, the Transport Layer Security protocol (TLS), enable a client and server to established a secure, encrypted connection over a public network. When you connect using SSL/TLS, the client authenticates the server before making a connection, and all data passed between Reflection and the server is encrypted.

template. A template includes all of the settings specific to documents. When you create a new document based on this template, it is configured identically, except that it prompts the user for a new name.

ticket lifetime. Refers to the period of time for which a ticket-granting ticket is valid. The user can request a ticket lifetime value when requesting a ticket-granting ticket. The server determines the maximum ticket lifetime. The default is eight hours (8h).

trusted host. A trusted host is one for which you hold the public key.

Trusted Locations. A trusted location is a directory that's designated as a secure source for opening files. By default, Reflection allows you to open documents only in directories specified as trusted locations in the Reflection settings.

URI (Uniform Resource Identifier). A string of characters that represents the location or address of a resource. URIs can be used to locate resources on the Internet or on an LDAP server.

Windows common application data folder. The application data folder is hidden by default. The default is `\ProgramData\`.

Windows personal application data folder. The personal application data folder is hidden by default. The default personal roaming application data folder is `\Users\`*`username`*`\AppData\Roaming\`.

Windows personal documents folder. The default on English systems is `\Users\` *`username`* `\Documents\`.