



Micro Focus Visual COBOL Development Hub 10.0

Release Notes

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK
<http://www.microfocus.com>

© Copyright 2024 Micro Focus or one of its affiliates.

MICRO FOCUS, the Micro Focus logo and Visual COBOL are trademarks or registered trademarks of Micro Focus or one of its affiliates.

All other marks are the property of their respective owners.

2024-06-26

Contents

Micro Focus Visual COBOL Development Hub 10.0 Release Notes	5
What's New	6
Rocket COBOL and Enterprise Extensions for Visual Studio Code	6
.NET Support	7
COBOL Language	7
Compiler Directives	7
Customer Experience Improvement Program	8
Enterprise Server	8
Enterprise Server Common Web Administration (ESCWA)	8
Enterprise Server Security	9
Interface Mapping Toolkit	9
Licensing Changes	9
Micro Focus Unit Testing Framework	10
OpenTelemetry	10
Significant Changes in Behavior or Usage	11
Resolved Issues	16
Known Issues	37
Other Issues Resolved in This Release	38
Unsupported or Deprecated Functionality	39
Additional Software Requirements	40
Installing Visual COBOL Development Hub	41
Before Installing	41
Downloading the Product	41
Installation on UNIX and Linux (Known Issues)	41
System Requirements for Micro Focus Visual COBOL Development Hub	42
Basic Installation	45
Installing Micro Focus Visual COBOL Development Hub	45
Advanced Installation Tasks	46
Installing as an Upgrade	46
Licensing Coexistence when Upgrading to Release 10.0	49
Micro Focus Visual COBOL Development Hub Installation Options	51
Installing Without Superuser Credentials	52
After Installing	54
Setting up the product	54
Enterprise Server Security Considerations	55
Configuring the Remote System Explorer Support	57
Configuring the firewall	58
Enabling SHIFT-JIS	59
Repairing on UNIX	60
Uninstalling	60
Licensing Information	61
To start Micro Focus License Administration	61
Installing licenses	61
Applying your license file	61
To obtain more licenses	61
Updates and OpenText Support for Micro Focus Products	62
Further Information and OpenText Support for Micro Focus Products	62
Information We Need	63
Creating Debug Files	63

Copyright and Disclaimer 64

Micro Focus Visual COBOL Development Hub 10.0 Release Notes

These release notes contain information that might not appear in the Help. Read them in their entirety before you install the product.



Note:

- This document contains a number of links to external Web sites. Micro Focus cannot be responsible for the contents of the Web site or for the contents of any site to which it might link. Web sites by their nature can change very rapidly and although we try to keep our links up-to-date, we cannot guarantee that they will always work as expected.
- Check the *Product Documentation* section of the [OpenText Support and Services Documentation Web site for Micro Focus products](#) for any documentation updates.

Product Overview

Micro Focus Visual COBOL Development Hub (Development Hub) is a part of the Micro Focus Visual COBOL product portfolio from Micro Focus which includes testing and developer productivity tools.

Development Hub is a companion of Visual COBOL for Eclipse. It enables the developers to use intelligent, integrated development tools in Eclipse while keeping the application source on a UNIX or Linux production-like server with access to middleware and test data. Developers get the power of Eclipse on their Windows or Linux desktop and can test their applications in a realistic environment without duplicating source code or emulating server behavior. With Visual COBOL, Micro Focus Visual COBOL Development Hub can be used for distributed development of COBOL for JVM applications.

What's New

Enhancements are available in the following areas:

- [Rocket COBOL Extensions for Visual Studio Code](#)
- [.NET Support](#)
- [COBOL Language](#)
- [Compiler Directives](#)
- [Customer Experience Improvement Program](#)
- [Enterprise Server](#)
- [Enterprise Server Common Web Administration \(ESCWA\)](#)
- [Enterprise Server Security](#)
- [Interface Mapping Toolkit](#)
- [Licensing Changes](#)
- [Micro Focus Unit Testing Framework](#)
- [OpenTelemetry](#)

Rocket COBOL and Enterprise Extensions for Visual Studio Code

[Back to Top](#)

The Micro Focus COBOL and Enterprise extensions for Visual Studio Code have been repackaged by Rocket Software on the Microsoft Visual Studio Marketplace.

- The Rocket COBOL extension for Visual Studio Code (formerly Micro Focus COBOL Extension for Visual Studio Code) provides COBOL edit, compile and debug support for Visual COBOL and Enterprise Developer users in Visual Studio Code.
- The Rocket Enterprise extension for Visual Studio Code (formerly Micro Focus Enterprise extension for Visual Studio Code) provides PL/I edit, compile and debug support for Enterprise Developer users in Visual Studio Code. This extension installs the Rocket COBOL extension.
- The Rocket JVM COBOL extension for Visual Studio Code (formerly Micro Focus JVM COBOL extension for Visual Studio Code) provides support for debugging JVM COBOL code in Visual Studio Code.
- The Learn COBOL extension for Visual Studio Code provides all training materials for the Micro Focus COBOL Fundamentals Training course.

New enhancements in this release are:

- Support for accepting command-line arguments in COBOL notebooks.
- New debug launch options - console and integrated Terminal support for platform specific values in the `launch.json` file.
- Support is available for fine-tuning the colors of different parts of the code in the editor via Visual Studio Code's `settings.json` file. This requires a minimum release 10.0 of Visual COBOL.



Note: These extensions are not included with the installer. They are available from the Microsoft Visual Studio Marketplace website. All of the extensions are available on Windows and Linux.

.NET Support

[Back to Top](#)

This release provides the following enhancements to .NET support:

- .NET COBOL projects now target .NET 8. You can use .NET 8 SDK or Visual Studio Code to build .NET 8 COBOL projects. Earlier versions of .NET are not supported.

COBOL Language

[Back to Top](#)

This release includes the following enhancements:

- The **FREE** statement - under the MF dialect, you can now free memory, allocated via the ALLOCATE statement, directly by using `FREE ADDRESS OF data-name`. This negates the need to specify a returning pointer during allocation (i.e. `ALLOCATE data-name RETURNING my-pointer`) and then freeing the pointer.
- **COBOL/Java interoperability** - the following features have been added to the COBOL and Java interoperability for native COBOL code:
 - Support for the use of dynamic length COBOL items when running under an MF dialect. See *Mapping COBOL Items and Java Types*.
 - User-defined exception handling when calling Java static methods. See *Example 5 - Exception Reporting When Calling Java Static Methods*.
- The **entry_point_mapper_disable_auto_aliasing** run-time tunable - this new tunable has been introduced to determine whether the Entry Point Mapping facility should *not* emulate the alias function of an IBM mainframe linkage editor, and instead generate a `COBRT173 Called program file not found in drive/directory` run-time system error.
- **Enterprise COBOL support** - the following enhancements provide greater compatibility with IBM Enterprise COBOL version 6.4:
 - The STRING and UNSTRING statements now support USAGE UTF-8 data items.
 - The ENCODING phrase of the JSON-GENERATE and JSON-PARSE statements is now supported.
 - The ENTRY-NAME and ENTRY-INTERFACE clauses of the Function-ID paragraph are now supported; however, these clauses are strictly documentary.
- **New MF Level** - this release includes a new default level (MF"23") of reserved words. See *Reserved Words Table* for words associated with this level.
- **Pointer dereferencing** - improvements have been made in the ability to dereference pointers using both the `DATA...AT` and `::` (colon-colon) syntax. See *Pointer Dereferencing*.

Compiler Directives

[Back to Top](#)

The following Compiler directive is new in this release:

- **ILPOINTER-REFERENCE** - Determines how a pointer used as a method parameter is passed if BY VALUE or BY REFERENCE is not specified as part of the parameter.

Customer Experience Improvement Program

[Back to Top](#)

Starting this release, the Customer Experience Improvement Program collects high-level, anonymous information on how Micro Focus products are used. The information collected includes product name and version, OS in use, and features used with the purpose to improve the products and, consequently, the customer experience.

Customer Experience Improvement Program participation is enabled by default. You can opt out with the help of the `mfceipconfig` command-line utility.

Enterprise Server

[Back to Top](#)

This release provides the following enhancements:

- Remote File Access - it is now possible to remotely access files using a configured Remote File Access (RFA) MFCS Connector. You can access ordinary files, cataloged datasets, and spool output. This also enables remote editing of COBOL data files using the new Data Tools utility. This enables you to download and upload files, datasets, and spool output locally or remotely using the existing Enterprise Server Security configuration. Various security features make this solution a more secure alternative to more generic solutions such as FTP and SSH.

Enterprise Server Common Web Administration (ESCWA)

[Back to Top](#)

This release includes the following enhancements:

- Catalog view has improved filtering options and now includes paging. A new **Load on navigation** check box enables you to filter based on the previously selected conditions. See *Catalog List* in the product Help.
- A new Configuration Report page enables you to visualize potential security vulnerabilities in the ESCWA and MFDS configurations. Each domain and configuration attribute combination has its own help dialog. See *Configuration Report* in the product Help.
- Role-based security configuration. You can now configure a users view of ESCWA. If a user does not require specific roles then you can hide corresponding pages and API. You can configure the role-based access from the **Role Options** page. Click **Security**, expand **ESCWA Configuration** followed by the **ESM**, and then click **Roles**. See *Role Options* in the product Help.



Note: Role-based security is an ESCWA only feature that works on top of existing product security.

- It is now possible to remove Locks, if necessary, to fix applications that are broken due to a lock that has not been removed. You can enable this feature from the **Locks** page. Click **Native > Monitor > Locks**, and then click **Remove Locks**. This functionality is controlled by the `casstop` resource entity in the `OPERCMDS` resource class. See *Locks* in the product Help.



Caution: Incorrectly removing locks can result in system instability and corruption or loss of data.

- Region verification - ESCWA can now verify the configuration of selected components for an enterprise server region. You can use this feature to identify potential start up or configuration issues for the selected region. The verification process uses the `casverify` utility to perform the verification action. See *Verify* in the product Help.

- Improved CICS resource navigation. Active resources can now be filtered by group and large sets of filtered data can be paged.
- The API return codes have been improved. Previously, when the region monitor and control APIs were called, they would return a HTTP 200 code, with the error specified in the JSON output. The return codes have been improved to give more information. You can configure the API to use the new or old behavior.
- The ESCWA user interface is now more responsive and can be used with a greater variety of smaller Web browsers.

Enterprise Server Security

[Back to Top](#)

This release includes the following enhancements:

- Enterprise Server security features provided by the VSAM External Security Manager (ESM) module are enabled by default. You will need to supply valid credentials when you interact with ESCWA, the Micro Focus Directory Server and regions in the browser based UI or in the IDE, use certain utilities from the command line, use TN3270 emulator to access regions, log into or with FileShare. See *After Installing > Enterprise Server Security Features* for details on how to configure this product.
- TLS Certificate Checking Utility - a new executable in the product that can be used to help diagnose problems with TLS certificates. It can check the validity of certificates, verify certificate chains, check that certificates and private keys match and check that a certificate contains a SAN that matches a provided hostname/address. Improves TLS usability by diagnosing TLS certificate problems. See *CertChecker Utility* for more information.
- The VSAM ESM Module, which provides file-based security for Enterprise Server is now a GA quality.
 - User authentication and resource authorization control can be enabled through a simple file-based security mechanism.
 - Security data can be imported from YAML or LDIF and exported to YAML for portability and ease of editing / scripting.
- Additional optional security features are available for HTTP and MFBINP conversations, for the Web Services and J2EE, Web, and Remote File Access conversation types. Listeners can be configured to require user authentication and/or to restrict access to specific types of requests. See *Enhanced Security for HTTP and MFBINP* for more information.

Interface Mapping Toolkit

[Back to Top](#)

This release provides the following enhancement:

- The `imtkmake -defmap` command now support the following new parameters that enhance the default mapping support for service interfaces - endpoint, method, and path.

Licensing Changes

[Back to Top](#)

- The SafeNet Sentinel licensing system that was available with previous releases of this product has been deprecated and is no longer available in release 10.0. This product also uses the Micro Focus AutoPass licensing technology which was introduced in release 8.0. Starting with release 10.0, AutoPass is the only licensing technology available in this product.

- The SafeNet Sentinel licenses are no longer supported, and you need to use AutoPass licenses starting with release 10.0. Contact your account manager to replace your existing SafeNet Sentinel with AutoPass licenses.



Note: Installing 10.0 on a machine where there are other Micro Focus products or versions installed that use SafeNet Sentinel licensing might result in some compatibility issues. While the 10.0 installation process has been designed to address such issues, you should be aware of the following scenarios and if any action might be required to ensure licensing works as expected. See *Advanced Installation Tasks > Licensing Coexistence when Upgrading to Release 10.0* in the *Installation* section.

Micro Focus Unit Testing Framework

[Back to Top](#)

This release includes the following enhancement:

- A new configuration file format has been introduced that enables you to use environment variables in your unit test code for tests that are compiled for more than one scenario. A portable environment file can provide environment variables for a test case that has been compiled in multiple ways (for Windows/UNIX, 32-bit/64-bit, etc...). See *Configuring the Run-Time System Environment* in your product Help.

OpenTelemetry

[Back to Top](#)

This release includes support for OpenTelemetry on UNIX platforms. OpenTelemetry provides observability of Enterprise Server applications by collecting telemetry data. You can configure OpenTelemetry to emit the information that you require and in a form that can be consumed by third-party monitoring software, such as Prometheus, Grafana, and Dynatrace. This can enable you to visualize processes and workflow performance and behavior.

Significant Changes in Behavior or Usage

This section describes significant changes in behavior or usage. These changes could potentially affect the behavior of existing applications or impact the way the tools are used.

- [Licensing Changes](#)
- [Significant Changes in Behavior or Usage - Enhancements](#)
- [Significant Changes in Behavior or Usage - Fixes](#)

Licensing Changes

[Back to the list](#)

- With release 10.0, the SafeNet Sentinel licensing technology has been deprecated. This can result in some compatibility issues if you install 10.0 on a machine where there are other Micro Focus products or versions installed that use SafeNet Sentinel licensing. While the 10.0 installation process has been designed to address such issues, you should be aware of the following scenarios and if any action might be required to ensure licensing works as expected. See *Advanced Installation Tasks > Licensing Coexistence when Upgrading to Release 10.0* in the *Installation* section.

Significant Changes in Behavior or Usage - Enhancements

[Back to the list](#)

The numbers that follow each issue are the Support Case Numbers followed by the Issue number (in parentheses).

- [Data Tools](#)
- [Enterprise Server](#)
- [SQL: Mainframe Batch Database Tools](#)

Enterprise Server

[Back to the list](#)

- Enterprise Server's PAM ESM Module now has a group-filter option that can be used to ignore all user groups that do not matching a specified pattern. See *PAM ESM Module Custom Configuration Information* in your product Help for more information.
3176983 (12500)
- In ESCWA, the **Enable Single Sign-On for Unsecured Resources** has been renamed to **Single Sign-On Behavior** which has three options:
 - **Disabled** - This disables all single sign-on including live enterprise server regions.
 - **Only Secure and Loopback** - This is the old 'default' behavior, single sign-on will be enabled for secured and localhost resources.
 - **Allow Insecure (All)** - Single sign-on will be enabled for everything. This list controls two boolean configuration attributes specified in the `commonwebadmin.json` file:
 - **InsecureAutoSignOn** - this is an existing attribute.
 - **DisableAutoSignOn** - this is a new attribute, if this is set to true then **InsecureAutoSignOn** will have no effect and all single sign-on will be disabled. If set to false then **InsecureAutoSignOn** will operate as before.
- In ESCWA, you can now set table column defaults for users. This can be configured from the column filtering option of the table in ESCWA. If an administrator has not set table defaults then the table
02663941 (658042)
- In ESCWA, you can now set table column defaults for users. This can be configured from the column filtering option of the table in ESCWA. If an administrator has not set table defaults then the table

columns displayed will match the ESCWA defaults. You can specify which users are able to configure default columns. This can be performed by modifying the **Table Column Configuration** security resource entity. See *Security Resources to Control ESCWA* and *API Access* in your product Help for more information.



Note: If **Table Column Configuration** is not specified then ESCWA will use the configuration specified for the **Common Web Administration** resource class.

02618280 (532051)

- The `casverify` utility has been improved with new functionality and additional verification stages. See *casverify* in your product Help for more information.



Note: The changes to its text and JSON output formats are incompatible with earlier versions.

(527008)

SQL: Mainframe Batch Database Tools

[Back to the list](#)

- The SQLTUL tool has been updated to enable you to specify that the return code (RC=04) for execution of non-SELECT * statements should match the mainframe DSNTIAUL return code. The default is to not match the return code, but to return RC=0. In addition, the `-r` option has been added to the `mbdtconfig` command to enable the same functionality from the command line.

02669700 (547020)

Significant Changes in Behavior or Usage - Fixes

[Back to the list](#)

The numbers that follow each issue are the Support Case Numbers followed by the Issue number (in parentheses).

- [Enterprise Server](#)
- [File Handling](#)
- [Interface Mapping Toolkit](#)
- [Micro Focus Directory Server](#)
- [Run-Time System](#)
- [SQL: Mainframe Batch Database Tools](#)

Enterprise Server

[Back to the list](#)

- When running with TRANCLASS active, TD Queue transaction triggering was not working.

02737664 (629076)

- ASSIGN INVOKINGPROG did not behave correctly when a CALL was involved.

02662244 (543070)

- A DPL over a SYNCLEVEL2 connection could result in an XA start being driven out of sequence resulting in a protocol error.

02583717 (477027)

- In a TRANCLASS enabled enterprise server region with a high volume of XA transactions, the logging overhead could cause performance degradation. This has been improved.

02560536 (468059)

- The PAC compatibility checks that run at startup have now been relaxed. Consistent platform and bitism are still checked, but product version checks are no longer carried out. The `ES_PAC_MIN_COMP_CHECK` environment flag has now been deprecated.



Note: Enterprise Server will still carry out record compatibility checks during start up.

(19756)

- The `statusCodes` flag has been added to some ESCWA API endpoints which can be used to enable ESMAC to return appropriate HTTP error status codes instead of embedding failure messages in successful responses. In a future product release, the new behavior will be enabled by default in the version 2 of the API and the flag will be removed. The version 1 of the API will maintain the current behavior.

02601489 (506061)

- ESCWA now limits the session timeout to 20 days. If an existing configuration is greater than that it will be limited to that value.

(665130)

- In ESCWA, the **Listener Properties** page now limits user inputs when the **smem** protocol is selected. Multiple host names are not permitted, and port selection is also not permitted.



Note: API functionality remains the same.

(665044)

- On UNIX platforms, the `casverify` utility no longer lacks the detailed file and folder path checking previously only supported on Windows platforms.

(407163)

- Runaway timeout was intermittently incorrectly calculated.

02529887 (468050)

- The JSON output format for the `casverify` utility has changed. Messages specific to `casverify` itself are no longer identified by "msgout" but under a "messages" array.

(570009)

- For Enterprise Server application failure reports and storage dumps generated by runtime errors, the RTS error code is now taken into account during `es-dump-limit` (`ES_DUMP_LIMIT`) processing. Runtime errors with differing error codes will now be treated as distinct.

02660093 (561067)

- The **Allow no-password signon for default users** property has been added to the ESCWA **Advanced Region Properties** page. If this property is set to `false`, an explicit signon request with no password matching an enterprise server default user account will no longer be treated as a no-password verify, and will instead result in a not authenticated failure.

02728103 (625033)

- The `es_default_security.yaml` file is now supplied with the product and is located at `%ProgramFiles(x86)%\Micro Focus\Enterprise Developer\etc` (Windows) or `$(COBDIR)/etc/vsam_esm` (UNIX). You can use this file as a template to configure the VSAM ESM Module. See the *VSAM ESM Module* topic in your product Help for more information.

(613052)

- Client connection to Micro Focus Directory Server (MFDS) would sometimes convert a fully qualified host name to just the simple host name. This could result in TLS connection issues if this did not exactly match the host names specified in the certificate.

02587914 (486048)

File Handling

[Back to the list](#)

- The Micro Focus file handler now passes correct information to the third-party file handlers for the implementation of the `FS_RENAME_FILE` routine.

02794472 (559042)

Interface Mapping Toolkit

[Back to the list](#)

- The base path is no longer part of the **Service name** field in the **Properties** dialog box of **REST Web service Deployment Server** tab. (It is only visible in the **Advanced Settings** of the service name.)

02795415 (651091)

Micro Focus Directory Server

[Back to the list](#)

- When starting or stopping an enterprise server region using MFDS or the ESCWA user interface, the `casstart` and `casstop /m` parameter would use the MFDS IP address rather than the host name, which could result in an issue if TLS certificates were used that required a particular host name.

02603383 (505074)

- An issue introduced Patch Update 1 resulted in ESCWA not listing all enterprise server regions for legacy import if they contained script data and the MF Directory Server was not sufficiently authorized to import script data.

(636060)

- The Micro Focus Directory Server (MFDS) **Start on System Start** enterprise server region option on the ESCWA General Properties page was not working because the **Automated Execution Control Enterprise Server Credentials** were not being applied correctly.

02795649 (652065)

- When exporting enterprise server regions registered in the MF Directory Server using XML format, regions for which the user did not have read/write access could also be exported.

(526005)

- Issues existed with importing enterprise server regions saved in JSON, XML, and Legacy format into a MF Directory Server, which resulted in incorrect listener states and counts.

(559058)

- You can now control the execution and update permission for an enterprise server region's start and stop, and on unrespondent scripts, by using a new LDAP Enterprise Server Administration security resource class **Scripts** entity. If this security resource entity has been specified with appropriate access control entries, the MFDS session will require Update permission in order for the authorized user to modify a region's script or to enable or disable it. In addition, for a script to execute, then you must specify Execute permission. See *Class - Enterprise Server Administration* in your product Help for more information.



Note: This is not a region restriction, but applies to the MFDS instance where the region is specified. If no security or MFDS Internal Security is configured for use then region scripts will not be executed nor will they be able to be modified. The Scripts resource is not a security resource created by default. It can be created by the ESCWA interface or other LDAP administration configuration tools.



Important: In future product versions, the access control that uses the Scripts security resource will be a requirement in order for any region's scripts to be executed or modified.

02822038 (499063)

- The default **UI Session Timeout** value for MF Directory Servers has changed from -1 (no timeout) to 600 seconds (10 minutes). The default value for the MF Directory Server **API Session Timeout** has been reduced from 3600 seconds (an hour) to 1200 seconds (20 minutes).

(628068)

Run-Time System

[Back to the list](#)

- The Java/COBOL application launcher - `cobjrun` - now supports Java command-line argument files. See <https://docs.oracle.com/en/java/javase/17/docs/specs/man/java.html#java-command-line-argument-files> for details on how these files should be constructed.

02744842 (636023)

- AIX 7.3 only: a dependence on Open XL C to create COBOL executables or shared objects has been removed.

02674547 (565031)

SQL: Mainframe Batch Database Tools

[Back to the list](#)

- An error that occurred in SQLUTB UNLOAD when the specified size of an LRECL was less than required for the row size has been fixed. The LRECL is now adjusted to accommodate the actual row size.

02445817 (612038)

- A problem with unloading GRAPHIC data using DSNTIAUL has been fixed.

02677441 (550046)

Resolved Issues

This section describes resolved issues in this release that resulted in product enhancements, and those that resulted in product fixes.

- [Resolved Issues - Enhancements](#)
- [Resolved Issues - Fixes](#)

Resolved Issues - Enhancements

[Back to the list](#)

The numbers that follow each issue are the Support Incident Numbers followed by the Defect number (in parentheses).

- [Enterprise Server](#)
- [Interface Mapping Toolkit](#)
- [Micro Focus Common Client](#)
- [Micro Focus Cryptographic Library](#)
- [SQL: Mainframe Batch Database Tools](#)

Enterprise Server

[Back to the list](#)

- You can now archive the auxiliary trace file by setting the `archive_auxiliary_trace` property to true. You can set this property in the **Enterprise Server Common Web Administration (ESCWA)** interface on the **Advanced Region Properties** page. See *Auxiliary Trace* in your product Help for more information.
(425091)
- In ESCWA, validation has been added to file path inputs to ensure they do not contain leading or trailing white space characters.
02513150 (446067)
- Exporting an enterprise server region as a JSON file will now be formatted.
02818032 (510031)
- Two new audit event codes have been added, 5 10 and 2 21. See *Audit Event Codes* in your product Help for more information.
02809915 (658081)
- In ESCWA, the **Password Change Enabled** check box has been added to the **Security Settings** page. Checking this enables you to change a users password when they log on.
02589857 (498029)
- In ESCWA, a new **Active XA Resources** widget has been added to the dashboard. See *Dashboard* in your product Help for more information.
02621260 (517076)
- In ESCWA, you can now remove locks for enterprise server regions that are part of a Performance and Availability Cluster (PAC). You need to be able to stop an enterprise server region in order to remove locks. The OPERCMDS(CASSTOP) resource will be checked.



Caution: Incorrectly removing locks can result in system instability and corruption or loss of data. You can contact Micro Focus Customer Support for more information and guidance on removing locks.

02659029 02869605 (545043)

- The `casverify` utility has been improved with a new verification stage to check connectivity to Scale Out Repositories (SOR) and key records for Performance and Availability Clusters (PAC) enabled enterprise server regions.

(549010)

- The `casverify` utility has been improved with new external security manager checks against configured default users and provided user credentials. Also, step names have become more concise, which might affect scripts consuming `casverify` output.

(609033)

- If the Micro Focus Common Client (MFCC) attempts to bind to an MFDS directory using configured credentials, and the credentials are rejected, it will retry the bind anonymously. This emulates the behavior of older product releases and is not a security weakness since it will only succeed against non-secured directories.

(673053)

- The password-expiration heuristic mechanism (**expiration-check** configuration setting) of the MLDAP ESM Module has been enhanced to improve accuracy under a number of conditions with various LDAP servers. Micro Focus recommends that customers using LDAP-based security for Enterprise Server with bind-mode user verification enable this setting as it results in more precise and accurate return codes from ESF Verify (user authentication) operations. See *MLDAP ESM Module Bind Rejection Heuristics* in your product Help for more information.

02547852 (472036)

- The **expiration-check** option of the MLDAP ESM Module now supports checking for the commonly-used LDAP user attributes `passwordExpirationTime` and `pwdChangedAt`, when attempting to determine whether a user bind was rejected due to an expired password. This improves the accuracy of the error codes returned when using LDAP-based security with bind-mode user verification.

02520274 (411002)

Interface Mapping Toolkit

[Back to the list](#)

- COBOL clients now correctly format an `x-www-form-urlencoded` JSON request body.

02495086 (402050)

- The generated COBOL Web service client proxy program now keeps the communication session open for the duration of potentially multiple service-invocation calls.

02441897 (385004)

Micro Focus Common Client

[Back to the list](#)

- When the Micro Focus Common Client (MFCC) needs to use MFDS to find the location of a service, it now by default tries to use the `readonly` account configured as part of the default Enterprise Server security to bind to MFDS. This is enabled through the `mf-client.dat` configuration file, and can be changed after installation. The effect of this change is that functions such as listing deployment listeners with the `imtkmake` command will typically work in a fresh product installation with no further configuration changes required.

(656131)

Micro Focus Cryptographic Library

[Back to the list](#)

- The TLS Certificate Checking Utility is a new executable that can be used to help diagnose problems with TLS certificates. It can check the validity of certificates, verify certificate chains, check that certificates and private keys match and check that a certificate contains a SAN that matches a provided hostname/address. It improves TLS usability by diagnosing TLS certificate problems.

(666106)

Resolved Issues - Fixes

[Back to the list](#)

The numbers that follow each issue are the Support Case Numbers followed by the Issue number (in parentheses).

- [Common Communications Interface](#)
- [Data Tools](#)
- [Documentation](#)
- [Enterprise Server](#)
- [Enterprise Server Auditing](#)
- [File Handling](#)
- [Interface Mapping Toolkit](#)
- [Micro Focus Directory Server](#)
- [Micro Focus License Administration](#)
- [Run-Time System](#)
- [SQL: COBSQL](#)
- [SQL: DB2 ECM](#)
- [SQL: Mainframe Batch Database Tools](#)
- [SQL: OpenESQL](#)
- [XML Support](#)

Common Communications Interface

[Back to the list](#)

- MRPI clients no longer experience high CPU usage when trying to contact a TLS enabled Micro Focus Directory Server (MFDS).

(474026)

- The CreateDemoCA script will now error with an informational message if the target directory does not exist.

(679011)

- Memory leaks occurred on outbound connections.

(632064)

Data Tools

[Back to the list](#)

- UNC paths were not properly resolved when loading data or structure files.

02819143 (673075)

- There was an issue with deleting multiple records of Line Sequential files simultaneously.

02542533 (425037)

- Previously, records located via the **Go To** action were not selected in the editor. This is now fixed.
02542696 (427048)
- The **Data File Tools Structure** view displayed incorrect values for binary data items that were explicitly defined with a number of storage bytes different to the default.
02649377 (536037)
- When inserting new records, the caret was always positioned at the end of the new record. This is now fixed.
02542581 (427045)
- In overwrite mode (toggled by Insert key) it was impossible to extend the length of text in fields. This also applied to functions like Find/Replace. This is now fixed.
02596359 (501005)

Documentation

[Back to the list](#)

- Searching the help for `special registers` now returns the main topic on special register usage.
(612069)
- Details of the CP pre-processors COPYINEXEC directive have been added to the documentation. Use this directive to determine whether CP treats COPY tokens in an EXEC statement as a COBOL COPY statement or part of the embedded language syntax.
02729687 (623036)
- The documentation for the READ statement has been corrected for rule 26 in the General Rules for Formats 1, 3, 4 and 5 (Sequential, Relative, and Indexed Files) section.
(489027)
- Dynamic length items are no longer restricted items to enclose in a JAVA-SHAREABLE block.
(666196)
- A formatting issue in the Usage Clause syntax diagram has been corrected - the THREAD-POINTER and typedef-name-1 elements are now showing correctly.
(505117)
- The parameters for library routine CBL_SUBSYSTEM have been updated in the product Help.
(386097)
- The documented restriction for the F run-time switch usage within .NET COBOL and JVM COBOL has been removed.
02720237 (613087)
- The Z run-time switch has been removed from the documentation.
(520009)
- The documentation now includes an additional rule for the DECLARE statement to point out that, unless explicitly initialized to a value, a DECLARED item is initially undefined.
(667190)
- A number of reserved and context-sensitive words have been added to the product in support of the latest ENTCOBOL enhancements; see the *Reserved Words Table* and *Context-sensitive Words Table* topics in the product help for full details.
(666134)
- An additional step has been added to the tutorial *Example 1 - COBOL Calling Java Static Method*, to ensure that the working directory is located on the CLASSPATH when running the example on UNIX platforms.
(553009)

- A typo has been corrected in the parameter definitions of the documented CBL_GET_PROGRAM_INFO routine.
(517025)
- The documentation has been updated to clarify some potentially undefined behavior when the cobtidy() function is invoked; see the *cobtidy()* help topic.
(637112)
- The documented Byte-stream library routines have now moved to a sub-section under the *Files and Filename Routines* section.
(610007)
- The documentation for the CALL statement has been corrected with respect to the LENGTH OF clause, which can now take a literal value when under the MF dialect.
02182932 (218025)
- The *File Handling Performance* documentation has been updated to reference the DATACOMPRESS and KEYCOMPRESS options, which can significantly improve performance.
02737405 (639069)
- The SORT documentation has been updated to include the BUILD synonym that is supported within the OUTFIL and OUTREC control statements.
02707437 (613023)
- The documented definition of MFFTP_PROCESS_TRAILS_ONGET control variable has been corrected to state it works in conjunction with LOCSITE (and not LOCSTAT).
02772554 (644097)
- Additional optional security features are available for HTTP and MFBINP conversations, for the Web Services and J2EE, Web, and Remote File Access conversation types. Listeners can be configured to require user authentication and/or to restrict access to specific types of requests. See *Enhanced Security for HTTP and MFBINP* in your produce Help for more information.
(635054)
- The option to associate an enterprise server region with a project has been removed from the Visual COBOL documentation.
00372693 (11386)
- The documentation covering the syntax options required for building the container demonstrations has been updated to include the hotfix option, when building demonstrations built from a patch update product.
02590001 (488005)
- The product documentation was missing a product name in the instructions for running a native COBOL application on a network server.
(550040)
- On UNIX platforms for 10.0, coherence is only supported for 64-bit machines.
(675057)
- The documentation now includes information on how to create a Certificate Authority (CA) trust store and how to set a password.
02767272 (643023)
- The JSON Processing tutorial in the documentation has had a few cosmetic updates.
(666207)
- The documentation has been updated to reference the level 78 item, MFU-GET-FILE, available in `mfunit.cpy`, that can be used to call the MFUGETF routine.
(9316)
- The documentation for the PROPERTY clause has been updated to explain how a property is exposed based on the setting of the ILARRAYPROPERTY directive.

00373023 (13206)

Enterprise Server

[Back to the list](#)

- The Mfsecrets AES provider now uses umask when creating directories.
(469050)
- Mfsecrets AES provider will now follow the umask when creating files
(464065)
- The Privacy Enhanced Mail file `CARootCerts.pem` has been updated.
(244065)
- On Ubuntu, running `CreateDemoCA.sh`, `CreateNewUserCerts.sh`, or `RevokeCertificate.sh` would not produce the required certificates and would fail with a script syntax issue.
(468007)
- ESCWA interactive API library request body documentation has been corrected for pipeline related endpoints.
(485045)
- Success message from CAS is now checked to return a success. Any message different to the successful cancel will now be interpreted as an error and ESCWA will notify as such.
(567043)
- ESCWA would crash when deleting a package or handler along with its associated service.
02594214 (489082)
- ESCWA now accepts fully qualified domain names for its bind address.
02493351 (450067)
- ESCWA will now return a unique message if the user if user has been revoked.
02808236 02862909 (651201)
- In ESCWA, on the **Services** page you can now delete parent services and associated packages in a single action.
02591547 (489045)
- In ESCWA and version 2 of its API, the DCT recoverable fields did perform correctly.
(561042)
- In ESCWA, an error would occur if non-ASCII characters were sent to ESMAC.
02729629 (625030)
- In ESCWA, the PO/PDS datasets were not loading.
02819576 (658003)
- In ESCWA, the SEPs logs were not displaying.
(652129)
- ESCWA interactive API V2 endpoints failed to operate correctly, including tracing and `tn3270Screen`. These have been fixed.
(485029)
- The ESCWA **XA Resource** page no longer has a notice that it is a technology preview feature.
02534474 (415107)
- ESCWA now allows Catalog Entries with DS Org set to GDG to have empty string to be submitted for Record Format through the API and it has been hidden by the API
(653208)

- In ESCWA, the documentation for the Web API contained errors that prevented client generation using OpenAPI. In addition, fields that were missing have been added and security and resource keys have been removed from version 2 of the API.



Attention: Micro Focus strongly recommends that you no longer use security and resource keys.

(453029)

- In ESCWA, the comparison of PAC strings were treated as case sensitive.

02761061 (638085)

- A problem that caused memory for `escwa.exe` processes to grow without falling back to normal levels has been fixed.

02735194 (629100)

- In ESCWA, validation has been added to multi-line file path inputs to ensure they do not contain leading or trailing white space characters.

02513150 (515022)

- In ESCWA, user token fields were treated as invalid if the stored value contained inconsistent capitalization.

02634935 (545054)

- In ESCWA, you can now remove locks if necessary. Contact Micro Focus Customer Support for more information and guidance on removing locks. See *Locks* in your product Help for more information. The `casstop` resource entity is checked as part of the OPERCMDS resource class. A user must have **Alter** permissions to do this, which are the same permissions required to stop a region.

(651022)

- User authorization is no longer logged by default and can be enabled in the ESCWA interface.

(682002)

- You can now configure ESCWA to audit request bodies. To enable this auditing, check **Audit Request Bodies** in **Tracing and Logging Settings**. This information is recorded in audit event code 5 10. See *Tracing and Logging Settings* and *Audit Event Codes* in your product Help for more information.

02605389 (525006)

- In earlier releases, the sample LDIF security definitions had incorrect definitions for the DOC*, TCP*, and URI* resources in the MFESMAC class. This resulted in access failures when attempting to view or modify those resource types in ESCWA for some administrative users when LDAP-based security was used and security rules were specified using one of the sample configurations.

(651189)

- The `mldap_esm` security manager will now load the appropriate threaded/non-threaded version of `libldap` which will result in the correct threaded/non-threaded LDAP library to be loaded.

(273023)

- On AIX, when using VSAM ESM and performing an ESF list resource action against an empty resource you will no longer receive an error.

(665081)

- When using `mfseconv` to export users, the **Audit** property was not exported correctly. In addition, when using `mfseconv` to convert LDIF to YAML the case of the **Mto** property for a user was not correct. These have been fixed.

(665201)

- The `esfadmin` command-line utility will now accept an ESM server URL of up to 256 characters in length. Previously this was limited to 80 characters.

(484061)

- The `mfseccconv` utility now sets a non-zero exit code if it encounters any serious errors, messages of error or severe error level are reported. If the new `--exit-codes` command-line option is specified, it sets exit code 3 if any severe errors are reported, 2 if any errors are reported, 1 if warnings are reported, and 0 if only informational messages are generated. This feature will assist in determining success or failure when running the utility in a script.

(653180)

- The `mfseccconv` export was creating incorrect YAML.

(652164)

- A number of modifications have been made to diagnostic messages to improve accuracy and relevance when users attempted to change their passwords under Enterprise Server, when the MLDAP ESM Module was used with bind-mode authentication.

02547852 (505042)

- An issue existed with the map CN configuration option for the DCAS conversation type.

02528628 (414079)

- If the configuration for a Security Manager using the MLDAP ESM Module explicitly disables Version 1 Authentication (the default behavior), this no longer incorrectly forces DSS wildcard processing to compatible mode.

02637403 (529091)

- Performing an `mfseccconv` import of a YAML file containing users with non-literal password verifiers will no longer cause those users to have an incorrect password.

(666125)

- Enterprise Servers MLDAP ESM Module can now detect the failure to contact an LDAP server for more types of network failures. Configure the connect timeout setting to permit the module to abandon hanging connection attempts after a specified time. If the redundant option is enabled for an enterprise server region (or ESCWA or MFDS) security, a connection timeout will let ESF fail over to another Security Manager; otherwise, it will let ESF fail the security request after the timeout expires, rather than hanging indefinitely.



Note: With this change, if a timeout is not configured the module will timeout a connection attempt after 2147483 seconds, a bit less than 25 days.

02004184 (193042)

- Under certain configurations the MLDAP ESM Module could fail to authenticate user credentials correctly, allowing users to sign onto Enterprise Server with incorrect passwords.

02652865 (537022)

- For security and SYSLOG AUDIT enabled enterprise server region, `mfdatatools2` no longer leaves File Descriptors with Syslog AUDIT permanently opened.

02792367 02806218 02882401 (652220)

- AIX files based on an ESDS file could not be viewed in ESMAC, ESCWA, or CFLE.

02580365 (486019)

- If a Distributed Program Link (DPL) targeting TXSeries resulted in a backout, this was not being signaled through EIBRESP.

02639307 (628005)

- When attempting to emit the message `CASKC0001E Transaction trn abend abcode. Backout Successful.` the CASSI process could trap with an RTS114 error.

02625044 (576015)

- When a distributed program link (DPL) originator executed a SYNCPOINT ROLLBACK the end of task processing would report an AEXJ abend.

02725418 (633017)

- The matching string was incorrectly built.
(297001)
- When `casgate` processed large volumes of concurrent work, the TCA control block could be left in an invalid state, resulting in the TCA being disconnected.
02609989 02612420 02618756 (509036)
- CASOUT requests can hang in server when SEPs are too busy.
02620485 (522007)
- When a 403 Forbidden was issued, the Web error program DFHWBEP was not called. This has been fixed
02833723 (665237)
- On a busy system, when multiple ITRs were created the KEY could sometimes be a duplicate, resulting in loss of an ITR. A unique key is now always created.
02615912 (517014)
- When using DISPLAY upon console, the buffer was truncated on the first `x00` value.
02793186 (653054)
- Concurrent SET FILE requests were resulting in SEP and enterprise server region crashes.
02629317 (528008)
- After a distributed program link had been executed a subsequent TS queue operation could result in a SYSIDERR.
02826408 (663078)
- When an enterprise server region was starting in a PAC, it could sometimes rollback an inflight transaction executing in another region.
02809622 02856124 (657012)
- Whenever trace flags are modified via ESCWA or `casutl`, a console message is now written to indicate the trace flags that are currently active.
(499017)
- If a pool thread in the `casras` process failed to access a record in the PSOR due to an error scenario that required the thread to reconnect, the thread did not retry to connect. The thread now retries the connection 10 times. This can be modified by setting `ES_SOR_RETRIES` to the required number of attempts. If the thread still fails to connect then a `CASRS2107E` console message will be generated.
02815996 02819419 02791959 02870114 (665003)
- The `casrdo` modules were initializing or handling the `cascookie` browser cookie incorrectly.
02713518 (589017)
- The FLENGTH operand is now initialized to 0 if the container no longer exists.
02794254 (652175)
- Files with more than 8 indexes were not being displayed in ESMAC.
(484021)
- The Historical Statistical Facility (HSF) `CASA_ECI_Function` now records the program name when a PGMIDERR abend occurs.
02406172 (362003)
- New ESMAC sessions did not redirect to the **System Sign On** page when the default user sign on was disabled on a secure enterprise server region.
02518847 (415043)
- A trap could occur in `casmgr` depending on the memory layout, because the memory type was not checked when processing a chain. This has been fixed
02835014 (665257)

- When a process died before responding to the process that issued an RPC wait, the recovery failed to dispatch the waiting process, resulting in a process hanging.
02671714 (561035)
- Invocation of a Tuxedo -hosted program using DPL and specifying a transaction ID was not working.
02538521 02644110 (419027)
- The terminator for custom field entries has been changed from # to x00. This is to prevent field entries from being truncated at #.
02737028 (629069)
- The `CASSI1452E` console message now correctly reports runtime errors that caused `casmfdbfh` initialization to fail.
02703834 (614008)
- The Internal Reader queue will now be installed in all enterprise server regions in a PAC, and not only on the first region starting the PAC.
02669519 02678257 (545089)
- Every time `casmgr` hard killed a process that was stuck after the threshold issued a kill, a dump was taken. If someone was formatting the dump at the same time, `casmgr` would be blocked trying to access the dump file for up to 10 seconds. A kill is now issued for all the stuck processes and only perform a single dump at the end.
02814032 (666034)
- If a `USERIDERR` occurred then the partner did not receive the error message.
02744133 (628170)
- When a `USERIDERR` occurred on a start transaction the socket failed to close. This has been fixed
02739278 (629094)
- When the `ENOMEM` error was reached after the maximum number of sockets were in use, the listener would not issue the `ACCEPT` call, resulting in a blocked listener.
02667973 (613088)
- When creating a resource the name was not being trimmed.
02667449 (542093)
- Using the `SET TRANSACTION` API did not publish changes to other enterprise server regions in the PAC.
02634669 02674657 02712535 (528029)
- A shared memory leak could occur during `castrc` recovery processing.
02568907 (474022)
- When a shared memory lock produces a dump, the lock is released before opening the dump file, and the lock is acquired afterwards.
02867469 (683131)
- An enterprise server region would fail to start if `FUTEX` was enabled.
02782113 (643047)
- The `casclsec` utility failed to receive the `userid`.
02636579 (526099)
- When a distributed program link passed a large channel, the receiving enterprise server regions buffer could overflow causing unpredictable behavior.
02600111 (517086)
- HTTP requests exceeding 32 headers to a Web Services and J2EE listener can cause a runtime error in `MFRHCGI`. This has been fixed. HTTP requests exceeding 64 headers to a Web Services and J2EE listener might be rejected with a 400 HTTP response status code with Too many request headers. in the response body.

- 02789436 (651069)
- A delay in transaction routing and DPL introduced by the fix for defect 401124 has been fixed.
- 02656673 02656960 (543009)
- On Linux platforms, the folder # will no longer be created under `/var/mfcobol/es/`.
- (669063)
- DPL interactions with a Tuxedo CRM server would trap during SL2 exchanges.
- 02667227 (543087)
- Issuing a program cancel with the no wait option in a PAC, left an orphaned record in the PSOR. This record is now cleaned up at the end of the command.
- 02674657 (615074)
- The FILE API response codes were not being propagated back to the remote system.
- 02785730 (648026)
- Incorrect auth calls were being made while using the DFED.
- 02628702 (529011)
- Alter or update privileges for a user are only checked when a user is performing an update action.
- 02619324 (515072)
- The code that matches TS queue instances with TSMODEL prefixes did not always return the closest matching prefix.
- (540013)
- An RTS 114 could occur in `cascd` or `casmgr` when the connection to the database used by MFDBFH was lost.
- 02575775 (486054)
- The copybook `dfhcbtct.cpy` has been updated to the latest version.
- 02821444 (667228)
- The 64-bit Dump Formatter incorrectly formatting trace point 4084 from `dfheserv`.
- 02599370 (506047)
- Improvements have been made to the checks for jobs waiting to be dispatched in an enterprise server region.
- 02596825 (503030)
- The console message `CASSI9051I` was not displayed correctly.
- (472003)
- Support for multiple system procedure libraries has been added.
- 02762877 (639081)
- LRECL was truncated when displaying the catalog dataset properties.
- 02632597 (528027)
- A delay in transaction routing and DPL introduced by the fix for defect 401124 has been fixed.
- 02645065 (526115)
- In ESCWA, an error caused uninitialized data to be entered into the file size in some cases where 0 should have been displayed.
- 02527126 02616594 (509029)
- The number of connected SEPs was truncated when the value was higher than 255.
- 02640448 (528100)
- When using the provided `TCPIPSERVICE(HTTPNSSL)` from `GROUP(DFHWEB)`, `CWBXN` would try to link to a program name only containing spaces as the `TCPIPSERVICE` had no URM defined.
- (645127)

- New traces have been added to differentiate between GLM, PAC, or LOCKDB locks.
(651046)
- An RTS 173 could occur in the `casverify` command-line utility during verification for the ESMQXA XA switch module.
(662068)
- If a network error occurred in one of the CASRAS threads but not in the PING thread, then the threads that contained the error would stop processing work.
02653594 02792419 (649048)
- Viewing the system trace table from ESCWA (by selecting **Trace X**) displayed invalid timestamps in all trace entries.
(566040)
- The find option in CEBR did not work correctly. This has been fixed
02803455 (657011)
- If an application performed a READ FILE ... UPDATE and then invoked a DELETE with RIDFLD() where the RIDFLD was different from that used in the READ, this would fail with an INVREQ.
02806458 (663049)
- If the buffer to display contained an `x 00` then the text was truncated.
02861717 (683119)
- When a user not accessible in the OS user database attempted to start an enterprise server region, a runtime error would occur in `cascfg`.
02659924 02782387 (543066)
- Previously, if a Configuration Manager property fails validation, the enterprise server region initialization would fail with a corresponding `CASCF0070E` console log error message. Now, in some situations the property value will be limited and identified by a `CASCF0071W` console log warning message.
02662199 (622019)
- DPL requests that interacted with Tuxedo CRM would result in a trap in the target during SyncPoint processing.
02690834 (600001)
- During an INVOKE SERVICE command, the name of the current channel might be incorrectly modified that is a GET CONTAINER with the CHANNEL option would return CHANNELERR.
02837778 (674022)
- ENDDATA was incorrectly sent when a client using http was disconnected.
02526457 (473050)
- On a busy system with active TRANCLASS, SEPs could hang if they did not receive a response to a request if some SEPs had died.
02646979 02671418 02751632 02680443 02894969 (547001)
- In ESMAC, user access to the **Server Information** page can be restricted using the **TABLE*** resource under **MFESMAC** in LDAP.
00368580 (13547)
- When running in a PAC, a RETRIEVE could incorrectly return an IOERR. This would occur if the transaction was initiated via a START using the TERMID and FROM options and the terminal was connected to an enterprise server region different to the one processing the transaction executing the START.
(477002)
- A PACs internal reader jobs were not dispatched when using disposition MOD.
02669519 (561052)

- The EIBRESP from the remote enterprise server region was not being propagated to the requester region.
(567053)
- When a SEP is killed before it can pick up work, the terminal was not notified resulting in a hung state.
02552505 (464090)
- The SET-TERMINAL performance has been improved. Shared memory is now used for an ENQ from a LOCKDB enterprise server region instead of using MFDBFH.
02797529 (651059)
- Authentication checks would fail when the ES_ESM_SECPRFX environment variable was enabled.
02628811 (527015)
- Viewing active Interval Control Elements (ICE) from ESCWA or ESMAC for a TRANCLASS enabled enterprise server region could unexpectedly fail, or result in a memory access violation in `castsc` if the Temporary Storage, Channels and Containers Control (TSC) trace flag was set.
02569568 (508026)
- If a SEP was terminated in the middle of writing to a TS queue, then an infinite loop could be encountered on all subsequent writes to that queue. This is a result of the queue control record not being updated. If this does occur then the first write will retry for a period before returning TIMEDOUT. All subsequent writes will function as normal.
02625902 (521033)
- Stage descriptions and step names in the `casverify` command-line utility have been updated to be more consistent and informative.
(662031)
- On UNIX, Enterprise Server stderr is redirected to `/dev/null` by default. If you want to redirect it to a file, set the ES_KEEP_STDERR environment variable to any value. This will create the `stderr.PID` file in the workarea.
02855699 (684081)
- Paths containing spaces were not correctly handled in enterprise server region configuration when using the `casverify` utility.
(550021)
- The token creation for the BROWSE CONTAINER commands (STARTBROWSE, GETNEXT, and ENDBROWSE) did not operate correctly.
(685021)
- A CFLE transaction incorrectly set the file to DISABLED when CLOSING.
02852107 (681023)
- Attempting to perform a DPL from TXSeries would fail due to unexpected PIP data included with the ATTACH.
02622825 02703317 (577002)
- An issue preventing Japanese localization from being displayed on the ESCWA **Advanced Region Properties** page has been fixed.
(389049)
- An error is now returned if a `castran /v` is attempted on a program that has a PPT specified.
(517043)
- When using the EXEC CICS INQUIRE TERMINAL API, the userarea and userarea len were not being returned correctly.
02767317 (644145)
- Displaying fixed record length files with deleted records on ESCWA and legacy ESMAC interface could have issues with paging and report an incorrect total record count.

(685076)

- The import and export of TST resources now supports Process Local and Exclusive queue types.

02757840 (640174)

- The incorrect length was used on query security when RESTYPE was used.

02852945 (679030)

- Starting a `cobesdebug` session with `type=J2EE` would result in a communications timeout error.

02594045 (504155)

- Attempting to dynamically update an XA Resource without a close string could result in an RTS114 within the `CASA_Update_XRM` service.

(653074)

- In a PAC environment, if a transaction had performed an XA prepare and not performed an XA commit or XA rollback while a new enterprise server region was starting, the recovery transaction started at the region start could result in an incorrect recovery of an inflight transaction. The process now checks that it is a true indoubt transaction rather than an inflight transaction.

02575529 (477030)

- Any nameless steps in preflight modules have now been titled appropriately.

(674050)

- The ESCWA v2 dynamic-config API produced a JSON error when a HTTP PUT request succeeds with further messages.

(653051)

- `SYSIDNT` was not retrieved correctly when added to the configuration manager.

02635287 (683088)

- Added option for regular JSON output to the `casverify` command line utility. See `casverify` in the product Help for more information.

(658063)

- The embedded template command `#INCLUDE` is now supported in DOCUMENT APIs.

02728038 (651024)

- When `XAID` is specified, `ISOLEVEL` is now set for the dynamic Oracle and DB2 switches.

(472008)

- If the `ESXAEXTCFG` exit module fails to load when `ESLOGGING` is enabled in the XA open string, then a `CASKC0025I` message will be displayed in the console log.

02725011 (623009)

- The PostgreSQL XA switch module now uses a valid SQL statement to test the current connection.

02721671 (618025)

- The XA recovery transaction failed when using `ES_XA_RECONNECT` and the connection to the Resource Module (RM) was lost, the transaction was started too many times which flooded the system.

02532560 (415184)

- XA resource without customization in the XA open string continues to open connection as-is when Micro Focus Vault support is enabled for other XA resources.

02671497 02675636 02819649 (547042)

- If a container that should have been created by the application was not found, then the error in `DFHJSON-ERROR` and `DFHJSON-ERRORMSG` failed to be returned. This is now fixed.

02801082 (652110)

- `mfsecrets` no longer displays unhelpful warning about config items not being found in ESCWA logs.

02543385 (425051)

- If `mfsecrets` fails to load the config file it now displays a more explicit error.
(662041)
- After performing a successful migrate, `mfsecretsadmin` will no longer produce an error message indicating it failed.
(661078)
- In ESCWA, previously the transaction count on the **Live Properties** page and API was incorrectly tied to the task number, which would reset when reaching 99999.
(683114)

Enterprise Server Auditing

[Back to the list](#)

- An issue occurred at shutdown when using TLS, this could result in socket closure before the peer had time to complete receiving.
(272016)

File Handling

[Back to the list](#)

- During a READ operation, the read closest op code now finds the next complete record from the relative byte address provided.
(387018)
- An issue, where programs that included the following copybooks failed to compile when using the `sourceformat(free)` directive, has been fixed:
`fsdatab.cpyfsdatabv2.cpyfsviewop.cpyfsviewopv2.cpyxfhcd3.cpy`
(403045)
- An issue has been fixed when initializing File Handling tracing when the `mfdas32` command is run.
(675076)

Interface Mapping Toolkit

[Back to the list](#)

- Web services using very large SOAP messages no longer throw a 153 (subscript out of range) runtime error.
02778746 (645015)
- COBOL client generation no longer fails due to the presence of escaped XML characters.
02730776 (629048)
- CICS Web Service requestor SOAP messages no longer contain extraneous namespace declarations.
02771747 (644034)
- Top-down generated CICS Web services now correctly handle mixed-content SOAP elements.
02809925 (651214)
- The `occurs` attribute is now unbounded on service interface fields for COBOL items that have an ODO clause and that are mapped using default mapping.
02614317 (519020)
- The presence of escaped XML characters sometimes caused COBOL client generation to fail.
02662184 (544055)

MFUnit Testing Framework

[Back to the list](#)

- An issue with COBOL Language Server failing to locate MFUPD_ and MFUWS_ prefixed files when compiling with the MFUnit Pre-Processor (mfupp) has been fixed.

(530030)

Micro Focus Directory Server

[Back to the list](#)

- Creating a new Communications Process could result in a duplication of an existing Communications Process instance value. This has been fixed. In addition, improvements have been made to enterprise server region **Validate** feature which now checks for and fixes duplicate instance values and Communications Process names that do not match the parent Enterprise Server name.

02627797 (528031)

- The Micro Focus Directory Server (MFDS) could sometimes crash when adding an External Security Manager (ESM) if no password was supplied.

(446038)

- A TLS-enabled Micro Focus Directory Server (MFDS) would become unresponsive when receiving requests from MRPI clients.

02552647 (465007)

- Setting Default Process UserID value as a UID rather than userid value caused the MFDS process to abend when using ESCWA to view enterprise server region data.

02604940 (515077)

- MF Directory Server would fail to start if `mfdscfg.xml` options file `bind_address` value was numeric rather than containing a valid hostname or IP address in standard format. Older versions of this file could contain either `127.0.0.1` represented as a 32-bit integer or `0` which represented listen on all available network adapters. MFDS now accepts either of these numeric address values.

02639711 (529085)

- When creating a Communications Process using the ESCWA API, any input hostname address value would always be set to `*`.

02670494 (547019)

- Fileshare server registrations in the MF Directory Server were not being preserved after the Directory Server was restarted and the **Save** legacy Micro Focus Servers option was checked.

02597483 (504062)

- In ESCWA, MFDS did not correctly support a shared memory (smem) listener configuration.

(677003)

- When starting enterprise server regions with ISC listeners, transient internal CCI servers with an MFNAME: prefix can appear in the MFDS or ESCWA user interface server list. To display these server types you must check the **Show System Server Types** option.

(484006)

- Fix issue with security configuration rollback if there was an issue verifying proposed configuration for MF Directory Server using ESCWA.

(665224)

- XRM openstring values were not saved to the configured vault when importing from a repository into the MF Directory Server.

(683175)

- In some circumstances, when importing legacy MF Directory Server configuration data the External Security Manager (ESM) password was not migrated to the Micro Focus Vault Facility correctly.

02574313 (525025)

- The mfActualEndpoint addresses for enterprise server listeners were not being updated or written to when using an XML file repository.
(495017)

Micro Focus License Administration

[Back to the list](#)

- An issue causing the CES daemon to crash has been resolved.
02816509 (617028)

Run-Time System

[Back to the list](#)

- Some native COBOL programs invoked via the `cobrun` trigger could display their command line parameters incorrectly.
02695958 (607020)
- Previously, the window position of COBOL programs executed with `runw/runmw` would not get restored correctly.
02560848 (453001)
- The RANDOM intrinsic function, when called from native COBOL programs, could sometimes return negative values when using large seed values.
02687376 (615064)
- Display issues when mixing COBOL ADIS displays with displays of a different type have been resolved.
02581162 (477021)
- Display issues, when mixing COBOL ADIS displays with displays of a different type, have been resolved.
02581162 (520022)
- Tab characters have been removed from one of the supplied copybooks: `cbltypes.cpy`.
02783984 (643089)
- Previously, running a COBOL program would erroneously fail with the `COBRT253 Cannot load file - unsupported format (Fatal)` error if `COBPATH` was explicitly set to not include the directory where the program was located. This has now been changed to return the `COBRT173 Called program file not found in drive/directory` error.
(588003)
- The tutorial instructions for COBOL calling Java static method (COBOL/Java Interoperability project) have been updated to specify the setting of the `COBSW` environment variable; this variable is required to address a display issue with the program output.
(567033)
- A new tunable - `entry_point_mapper_invalid_path_error` - which is off by default, has been added to control whether the COBOL Run-Time System should report an error if the `ENTRYNAMEMAP` environment variable refers to invalid/non-existent filename and directory paths.
(589018)

SQL: COBSQL

[Back to the list](#)

- COBSQL now correctly handles host variable arrays that require COMP/COMP5 conversion.

- 02668849 (543111)
- COBSQL has been updated to correctly handle an END-PERFORM problem caused by the new swap byte logic.
- 02668849 (562025)
- COBSQL has been updated to support sign conversion of CHARSET ASCII + SIGN EBCDIC.
- 02683191 (573002)
- COBSQL has been modified such that it no longer inserts group information in the EBCDIC conversion statement when the group variable is a FILLER.
- 02555993 (442071)
- COBSQL was updated to correctly handle EBCDIC conversion of EXEC SQL OPEN USING statements.
- 02804887 (651165)
- COBSQL has been updated to handle EBCDIC conversion of numerical values contained within redefined group variables.
- 02584237 (481010)
- COBSQL has been updated to fix compilation issues related to ALPHA-LIT-CONT directive support.
- 02594669 (489083)
- To correct a compile problem caused by redefined variables, COBSQL has been updated to closely track group variable information while determining which variables to convert.
- 02570841 (464033)
- COBSQL now properly handles the EBCDIC conversion of FETCH FIRST/NEXT statements.
- (649057)
- COBSQL has been updated to fix a swap-byte conversion issue that occurred because an SQLCODE=100 was returned after a multi-row FETCH.
- 02702058 (596010)
- COBSQL has been modified in this release to handle EBCDIC conversion of FETCH ROWSET statements.
- 02687410 (637117)
- COBSQL has been updated to properly terminate EXEC SQL statements that are replaced by dummy lines during SYBASE precompilation.
- 02722549 (625013)
- COBSQL now correctly handles EBCDIC conversion of EXEC SQL statements that contain group items as host variables.
- 02791368 (649037)
- COBSQL now recognizes the NOAMODE directive and handles it correctly at run time.
- 02592714 (516075)
- COBSQL now correctly handles source lines that contain a comma in column 8 immediately followed by a COMP host variable.
- 02675814 (547024)
- COBSQL was updated to support ENTRY statements broken into multiple lines.
- 02426309 (374014)
- COBSQL was updated to use heap instead of an array to handle redefined variables.
- 02666211 (71231)
- COBSQL has been modified to handle periods in column 72 when the next line is empty.
- 02485117 (414080)

- COBSQL was updated to handle inline comments after END-EXEC token.
02624353 (520008)
- COBSQL now generates run-time logic correctly for signed numeric data items.
02811569 (658027)
- COBSQL now correctly handles signed numeric data items in a group.
02811569 (656026)

SQL: DB2 ECM

[Back to the list](#)

- A problem that occurred when compiling a program using the DB2 ECM caused a -1309 SQLCODE compiler error instead of a connection pop-up dialog.
02354465 (503026)
- A problem using an mfaemon resource for connection credentials compiling a program using the DB2 ECM has been fixed.
02354465 (643020)
- DB2ECM now compiles without problem when the HOSTVAR directive is used.
02686034 (564020)
- The DB2 ECM produced a connection dialog box instead of automatically connecting when the mfaemon was not started and mfaclient.ini contained valid database connection credentials. This has been resolved.
02354465 (644030)

SQL: Mainframe Batch Database Tools

[Back to the list](#)

- A problem that prevented SQLUTB from generating a correct COND CODE when one job step contained multiple commands has been fixed.
02626837 (519044)
- A problem with reading wrongly cataloged datasets with incorrect LRECL has been fixed.
02565909 (489096)
- SQLUTB has been updated to support constant field specifications.
02596145 (499004)
- A problem that sometimes occurred when using the SYSPUNCH generated by SQTUL for SQLUTB LOAD has been fixed.
(504040)
- A problem loading and unloading Zoned DECIMAL data using SQLUTB has been fixed. The NULLIF defined on column (name) is supported in this release for SQLUTB LOAD.
02348281 (319036)
- MINVALUE and MAXVALUE in the partition definition of a table in DB2 LUW are now supported.
02552457 (442029)
- A problem that occurred when converting between IEE754 format and IBM370 format for float data types on Linux has been corrected so that MBDT LOAD and UNLOAD work correctly for FLOAT data types.
02848184 (673083)
- A problem conforming the mainframe COND CODEs for SELECT * and SELECT individual columns has been fixed.

- 02608857 02564044 02766263 (504179)
 - A problem that occurred when executing SQLTUL to unload data in any sequence of jobs with and without PARM(SQL) has been fixed.
- 02708425 (619015)
 - A problem with using STATISTICS TABLE(ALL) INDEX(ALL) syntax in SQLUTB load has been fixed.
- 02630363 (529003)
 - A problem with SQTUL/DSNTIAUL that sometimes occurred when changing a dataset from SYSPUNCH to DUMMY has been fixed.
- 02563262 (455025)
 - The MBDTConfig message file is now shipped with Enterprise Server and COBOL Server.
- 02861596 (683077)
 - A problem with SQLUTB UNLOAD using SQL 2 operators in one logical expression in the WHEN clause has been fixed.
- 02585747 (482004)
 - When DB2 LUW detects an invalid datetime format with SQLCODE: -99999, SQLSTATE: 22008 - CLI0113E SQLSTATE 22007, error rows are now properly discarded. Processing continues and the COND CODE is set to 04.
- 02565241 (458002)
 - A problem with SQLTUL that caused an error when using UTF-8 encoding and unloading a CHAR() column containing PostgreSQL DBCS characters has been fixed.
- (515069)
 - A problem with the MBDT Configuration utility that caused issues when setting the -t option on UNIX has been corrected by updating MBDT with the new -g option, used to create and access the OpenESQLConfig.ini in the \$COBDIR/etc directory on UNIX platforms only.
- (542087)
 - A problem that occurred when executing SQLUTB jobs against DB2 for z/OS has been fixed.
- 02627157 (644114)

SQL: OpenESQL

[Back to the list](#)

- The native SQL runtime sometimes hung when it encountered the EXEC SQL ROLLBACK TO SAVEPOINT command. This has been resolved.
- 02565661 (469019)
 - A problem that caused an unwarranted rollback when the last SQL statement issued was a commit or rollback, and the next SQL statement was a disconnect has been resolved.
- 02731137 (628044)
 - OpenESQL now handles EBCDIC application correctly when the AMODE(31) directive is used in a 64-bit environment.
- 02541041 (454020)
 - DSNREXX now handles multiple SQL Statements correctly and without corrupting memory.
- 02599095 (504116)
 - A problem that prevented the OpenESQL runtime from releasing all pinned .NET objects for MFSQLMESSAGETXT has been fixed.
- 02690852 (612080)
 - OpenESQL has been updated to support user IDs containing a dot.
- 02637077 (525103)

- A problem with incorrectly cleaning up the ODBC environment sometimes caused OpenESQL to throw a memory access violation error. In this release, the ODBC environment is cleaned up such that this error no longer occurs.
02742293 (630097)
- WITH RETURN cursors are now opened as KEYSET type instead of DYNAMIC type.
02541903 (461001)
- A compiler error that was caused when using the SQL(GEN-SQLCA) directive without separately defining SQLSTATE in program code has been fixed.
02743040 02794285 (629124)
- The ODBC ECM error code 12 was sometimes returned during a compile with SQL directives when processing an interface.
02543269 (425092)
- A problem that sometimes caused the OpenESQL runtime to leak memory when handling threads has been fixed.
02646010 (531005)
- The THREAD=ISOLATE SQL compiler directive option now works correctly when a native connection is used by a managed program running in the same thread.
02670859 (625018)
- The Oracle RM switch module now supports Oracle Client version 21c.
02850631 (673121)

XML Support

[Back to the list](#)

- XMLPARSE now correctly handles small XML instance documents on the AIX platform.
02799668 (652088)
- XML PARSE has been updated to properly handle XML instance documents with a large number of content characters within tags.
02575649 (472007)
- The XMLPARSE feature is now available in the Enterprise Server for Stored Procedures product.
02822761 (663037)
- XML READ now performs much faster when a big OCCURS value is used in the XML data-item.
02630023 (525082)

Known Issues

Refer to the *Known Issues and Restrictions* topic in the *Product Information* section of your product Help.

In addition, note the following:

- JVM COBOL applications that run on AIX7.3 using Java versions 21.0.1 or 21.0.2 (IBM Semeru Runtime Open Edition) show intermittent errors in the Java runtime ('java.lang.SecurityException: SHA-256 digest error') resulting in the application not running as expected. The product `.jar` files are signed.
- In Visual COBOL 4.0 and 5.0 in an extremely small and limited set of cases, an issue could occur with running `.NET` executables and `.dll` files, or JVM `.class` files, created with an earlier version of the product. This issue only occurred if:
 1. The application performs an IS NUMERIC condition test on a variable declared with USAGE NATIONAL.
 2. The application has been created with Visual COBOL 3.0 or earlier, then executed in Visual COBOL 4.0 or 5.0.

In these rare cases, the IS NUMERIC test could provide the wrong answer.

In order to resolve this issue, in Visual COBOL 6.0 and later, the `.NET` COBOL and JVM COBOL run-times reject any program using IS NUMERIC on a NATIONAL item which was compiled with a version 5.0 or earlier of the product. You receive a "missing method" exception. To resolve the issue, you need to recompile any programs that use this construct in the newer versions of Visual COBOL.

Program that do not use NATIONAL data, or those that have been recompiled in Visual COBOL 6.0 or later are not affected.

Other Issues Resolved in This Release

The numbers listed are the Support Incident Numbers followed by the Issue number (in parentheses).

- 02556886 (468003)
- (662117)
- 02537488 (453046)
- 02624110 (520012)
- 02723517 (618034)
- 00363234 (28048)
- 00477923 (61180)
- 02822038 (508052)
- 02394824 02778550 (351052)
- 00373450 02406104 (11527)
- (61096)
- (442036)
- 02823160 (675050)
- 02725405 (628033)
- 02780781 (647035)
- 02743825 (629142)
- 02686079 02733133 (629006)
- 02600111 (597005)
- 02583111 (485001)
- 02783874 (648018)
- 02646617 (540015)
- (513014)
- (568005)
- 02677554 (560014)
- 02730120 (628029)
- (649040)

Unsupported or Deprecated Functionality

This section includes information about features or functionality that are not supported.

- The SafeNet Sentinel licensing system has been deprecated. This product uses the Micro Focus AutoPass licensing technology. Contact your account manager to replace your existing SafeNet Sentinel with AutoPass licenses. Also, see *Advanced Installation Tasks > Licensing Coexistence when Upgrading to Release 10.0* in the *Installation* section in your product Help.
- The HOSTSIGNS Compiler directive is no longer supported. Micro Focus recommends that you use the following Compiler directives instead: SIGN-FIXUP, HOST-NUMMOVE, and HOST-NUMCOMPARE. This is a change since version 3.0 of this product.

Additional Software Requirements

To ensure full functionality for some features, you might be required to obtain and install additional third-party software.

[Click here](#) to see this information on the Product Documentation pages on OpenText Support for Micro Focus Products, in the product Help for Micro Focus Visual COBOL Development Hub.

Installing Visual COBOL Development Hub

Before Installing

Downloading the Product

1. Log into the Software Licenses and Downloads (SLD) site at <https://sld.microfocus.com/mysoftware/download/downloadCenter>.
2. Select your account and click **Entitlements**.
3. Search for the product by using any of the available search parameters.
4. Click **Show all entitlements**.
5. Click **Get Software** in the Action column for the product you want to download or update.

In the **File Type** column, you see entries for "Software" for any GA products, and "Patch" for any patch updates.

6. Click **Download** on the relevant row.

Installation on UNIX and Linux (Known Issues)

Installing on Red Hat 8.x s390

On Red Hat 8.x s390, the RPM non-root install method is not supported due to errors given by cpio. You receive the following messages:

```
error: unpacking of archive failed on file /usr/lib/.build-id/1b/af99f26c6b4c00ca499a3199a574b73aeb3854;6092b79c: cpio: symlink failed - No such file or directory
error: Micro_Focus_cobol_server-7.0.0.0-100700.s390x: install failed
```

As a result, the installation in this scenario is incomplete.

Installing while using AFS/Kerberos authentication

If you are using AFS/Kerberos authentication to log onto your Linux system then you need to ensure you have a local user ID which SOA and Visual COBOL components of the product can use. This user ID must be set up prior to running the installer. When running the installer you need to specify - `ESadminID=[User ID]` on the command line so it is used by the installer.

License Server

You need to configure the computer hostname to ensure the license server will start properly.

To avoid performance issues, "localhost" and the computer hostname must not both be mapped to IP address 127.0.0.1. You should only map "localhost" to IP address 127.0.0.1.

The following is an example of how to specify these entries correctly in the `/etc/hosts` file:

```
127.0.0.1 localhost.localdomain localhost
IP machinelonghostname machineshorthostname
```

where *IP* is the unique IP address of the computer in xx.xx.xx.xx format.

System Requirements for Micro Focus Visual COBOL Development Hub

Hardware Requirements

The disk space requirements are approximately:

Platform	Installer type	Setup file size	Disk space required for the installation	Disk space required for running the product	Licensing technology
x64 running Amazon Linux 2	Micro Focus	657 MB	2.63 GB	1.31 GB	90 MB
Amazon for Docker	Micro Focus	656 MB	2.86 GB	1.31 GB	90 MB
POWER running AIX	Micro Focus	775 MB	3.1 GB	1.55 GB	102 MB
System Z running Red Hat Linux	Micro Focus	485 MB	1.94 GB	970 MB	113 MB
x86-64 running Red Hat Linux	Micro Focus	919 MB	3.68 GB	1.84 GB	91 MB
64 running Red Hat Linux	Micro Focus	539 MB	2.16 GB	1.08 GB	91 MB
64 running Red Hat Linux	Micro Focus	213 MB	852 MB	426 MB	91 MB
Red Hat for Docker	Micro Focus	659 MB	2.64 GB	1.32 GB	91 MB
x86-64 running Solaris	Micro Focus	724 MB	2.90 GB	1.45 GB	33 MB
System Z running SUSE SLES	Micro Focus	459 MB	1.84 GB	918 MB	79 MB
x64 running SUSE SLES	Micro Focus	661 MB	2.64 GB	1.32 GB	86 MB
x64 running Ubuntu	Micro Focus	661 MB	2.64 GB	1.32 GB	86 MB
SUSE for Docker	Micro Focus	659 MB	2.64 GB	1.32 GB	86 MB
Ubuntu for Docker	Micro Focus	659 MB	2.64 GB	1.32 GB	86 MB
x86-64 running Rocky Linux	Micro Focus	919 MB	3.68 GB	1.84 GB	91 MB


Platform	Installer type	Setup file size	Disk space required for the installation	Disk space required for running the product	Licensing technology
Rocky Linux for Docker	Micro Focus	659 MB	2.64 GB	1.32 GB	91 MB
x86-64 running Oracle Linux - Red Hat Compatibility Kernel	Micro Focus	865 MB	3.46 GB	1.73 GB	50 MB

Operating Systems Supported

For a list of supported operating systems, see *Supported Operating Systems and Third-party Software* in your product documentation.

On some platforms, there is only a 64-bit version of this product. 64-bit versions of the product support compiling to and running 64-bit programs only.

Software Requirements

 **Note:** This product includes OpenSSL version 3.0.8.

The following topic lists the software requirements for Micro Focus Visual COBOL Development Hub.

- [Software required by the setup file](#)
- [Libraries required by the setup file](#)
- [Software required to run the product](#)
- [Required environment variables](#)
- [License Manager requirements](#)

Software required by the setup file

- The "awk", "ed", "ps", "sed", "tar", "sed" and "which" "tar" utilities must be installed and added to the PATH.
- On AIX 7.2 and 7.3, the installer requires the Open XL C/C++ 17.1 Clang C++ compiler. You need to install the Open XL C/C++ 17.1 runtime environment and utilities package.
- If SELinux is installed and you plan to use anything other than core COBOL functionality, or plan to use Enterprise Server within an environment with ASLR enabled, the "SELINUX" configuration must be disabled. To do this, set `SELINUX=disabled` in `/etc/selinux/config`.
- Xterm, the terminal emulator for the X Window System, is part of your UNIX/Linux distribution but is not always installed by default. Use your UNIX/Linux installation media to install it.

Libraries required by the setup file

The following table lists the required libraries for Red Hat and SUSE Linux platforms. The setup file checks that both the 32-bit and 64-bit libraries listed below are installed on both 32-bit and on 64-bit Operating Systems for this product to install and work correctly.

If installing on a 64-bit OS, the 32-bit libraries are not installed by default and must be installed before you start the installation.

The following table shows which of the required libraries are not installed by default on the specified platforms - X indicates the libraries are missing.

Library	Platform								
	32-bit	64-bit	s390	SUSE 12	SUSE 15	Red Hat 7	Red Hat 8	CentOS 7	Ubuntu 18 and 20
glibc ¹	X	X	X			X	X	X	
libgcc	X	X	X			X	X	X	
libstdc++	X	X	X			X	X	X	
glibc-devel	X	X	X			X	X		
gcc ^{2,3}	X	X	X	X	X	X	X	X	
cpp ²		X				X	X	X	
libgc1c2		X							X

- Libraries marked with an 'X' are not included in the platform and need to be installed separately.
- ¹On 64-bit Red Hat 7, you only need to install glibc-2.17*.x86_64 and glibc-2.17*.i686.
- ²On Red Hat, these libraries are required to enable COBOL to compile.
- ³On Red Hat, only the 64-bit gcc libraries are required.

Visit the [Red Hat Web site](#) for more information.

Software required to run the product

- Java 1.8 (64-bit) or later is required to run Micro Focus Visual COBOL Development Hub. The recommended version is Adoptium's OpenJDK Temurin 17 (LTS) with HotSpot. You can download Adoptium's OpenJDK Temurin 17 (LTS) with HotSpot from [Adoptium's Web site](#) and unpack the archive anywhere on your machine.

Required environment variables

- Set the JAVA_HOME environment variable. When installing the product, set this variable to a 64-bit Java installation or the installation terminates. For example, execute the following:

```
export JAVA_HOME=java_install_dir
```

where *java_install_dir* is the path to the JAVA installation directory such as */usr/java/javan.n*

- Add \$JAVA_HOME/bin to your system PATH variable. To do this, execute:

```
export PATH=$JAVA_HOME/bin:$PATH
```

- You need to set the LANG environment variable to pick up localized messages. If you do not set it as specified here, the installation will run but you might experience unexpected behavior from the installer.

The LANG settings are English and Japanese only so set it to one of the following locales:

```
C, default, en_GB, en_GB.UTF-8, en_US, en_US.UTF-8
```

```
ja_JP, ja_JP.SJIS, ja_JP.UTF-8, ja_JP.eucJP, ja_JP.eucjp, ja_JP.sjis, ja_JP.ujis, ja_JP.utf8, japanese
```

You can set LANG before running the setup file as follows:

```
export LANG=C
```

Alternatively, add it to the start of the setup command line:

```
LANG=C ./setupfilename
```

See *Using the LANG Environment Variable* for details.

License Manager requirements

- For local servers, you do not need to install the Micro Focus License Administration tool separately, as the setup file installs a new Visual COBOL client and a new licensing server on the same machine.
- If you have any network license servers, you must update them before you update the client machines.
- If you are upgrading from Visual COBOL release 2.2 or earlier, uninstall the license manager before installing the product.

You can download the new version of the license server software by following these steps:

1. Log into the Software Licenses and Downloads (SLD) site at <https://sld.microfocus.com/mysoftware/download/downloadCenter>.
2. Select your account and click **Downloads**.
3. Select a product and a product version from your orders.
4. In the list of software downloads, locate the **License Manager**.
5. Click **Download** to download an archive with the installers.
6. Run the installer suitable for your Operating System to install License Manager on your machine.

Basic Installation

The instructions in this section apply when you are performing a basic installation of this product for the first time. If you are an administrator, you can perform a basic installation on a local machine before performing a more advanced installation when rolling out the product to developers within your organization.

For considerations when installing this product as an upgrade, for additional installation options or non-default installations, see *Advanced Installation Tasks* in your product Help.

Installing Micro Focus Visual COBOL Development Hub

Micro Focus offers two types of installers on UNIX and Linux - a proprietary Micro Focus installer for installing on UNIX and Linux and a standard RPM (RPM Package Manager) installer for installing on Linux. See your product Help for instructions on how to use the RPM installer.

Before starting the installation, see *Software Requirements*.

These are the steps to install this product using the Micro Focus installer:

1. Give execute permissions to the setup file:

```
chmod +x setup_visualcobol_devhub_10.0_platform
```

2. Run the installer with superuser permissions:

```
./setup_visualcobol_devhub_10.0_platform
```

If you don't run this as superuser you will be prompted to enter the superuser password during the installation.



Note: On Ubuntu, the prompt for superuser password is not available. On this platform you must either log in as root or use the `sudo` command to get root permissions before you run the installer.

The COBOL environment is installed by default into `/opt/microfocus/VisualCOBOL`, (COBDIR).

Enterprise Server System Administrator Process

During the installation process, the installer configures the product's Enterprise Server System Administrator Process User ID. The Process User ID will be the owner of all Enterprise Server processes except the one for the Micro Focus Directory Server (MFDS). The Directory Server process (Enterprise Server Administration) runs as root as this allows it to access the system files and ports.

All Enterprise Server processes you start from Enterprise Server Administration run under the Process User ID which can affect the file access and creation.

You must supply the user ID at the command line - specify `-EsadminID=[ID]` as part of your command.

By default, the installer uses the login id of the user that runs the installer for the Process User ID. To change the user id after you complete the installation, execute `$(COBDIR)/bin/casperm.sh` and follow the onscreen instructions.

AutoPass Licensing considerations

- The installation of this product could affect the AutoPass licensed components running on your machine. During installation, the licensing shuts down to allow files to be updated. To ensure the processes running on your machine are not affected, you need to use the `-skipautopass` option, which skips the installation of AutoPass:

```
./setup file -skipautopass
```

- To protect the AutoPass installation from accidental updating, you can create an empty file named `SKIP_AUTOPASS_INSTALL` in `/opt/microfocus/licensing` as follows:

```
touch /opt/microfocus/licensing/SKIP_AUTOPASS_INSTALL
```

While the file is present, the AutoPass installer does not make changes to the installation or shutdown the running license daemons. If licensing needs to be updated later, you can rerun the `MFLicenseServerInstall.sh` from within the `$(COBDIR)/licensing` folder with the force command line option:

```
cd $(COBDIR)/licensing
./MFLicenseServerInstall.sh force
```

Advanced Installation Tasks

This section includes instructions about how to perform a non-default installation, install this product as an upgrade, or about how to install the additional components.

The advanced installation tasks include:

- *Installing as an Upgrade* - included in these Release Notes
- *Command line installation options* - included in these Release Notes
- *Installing using an RPM installer on Linux* - available in the product Help and in the Micro Focus Infocenter

[Click here](#) to see this information on the Product Documentation pages on Micro Focus OpenText Support for Micro Focus Products.

Installing as an Upgrade

This release works concurrently with the previous version of Micro Focus Visual COBOL Development Hub, so you do not need to uninstall it. See the rest of this topic for considerations when installing alongside older releases.

Install the latest version in a different location and set the environment to point to it. To do this, run the Micro Focus Visual COBOL Development Hub installer with the `-installlocation` option:

1. Execute the following command:

```
./InstallFile -installlocation="/opt/microfocus/VisualCOBOL"
```



Note: You can use variables when specifying an absolute path for `-installlocation`. For example, the following examples are equivalent:

```
-installlocation="/home/myid/installdir"
```

```
-installlocation="$HOME/installdir"
```

2. Execute `cobsetenv` to set the environment and point to the new install location:

```
. <product-install-dir>/bin/cobsetenv
```



Note: `cobsetenv` is only compatible with POSIX-like shells, such as `bash`, `ksh`, or `XPG4 sh`. It is not compatible with C-shell or pre-XPG4 Bourne shell.

Preserving the Licensing Configuration Alongside Older Releases

The following is required when you use release 10.0 alongside earlier supported releases of this product on the same machine. The licensing configuration file has changed in release 10.0 and you need to ensure that the older releases do not overwrite it as this can result in issue with licensing and auto-start setup.

You can do this in one of the following ways:

- Execute the following after you install release 10.0:

```
touch /var/microfocuslicensing/SKIP_SAFENET_INSTALL
touch /opt/microfocus/licensing/SKIP_AUTOPASS_INSTALL
```

- Alternatively, when installing releases earlier than 10.0, use the following command line options during the installation:

```
-skipsafenet -skipautopass
```

This skips the license installation step for those releases and preserves the licensing configuration for release 10.0.

Preserving Product Configuration

The following information applies when you are upgrading from releases 8.0, 9.0, and above.

If you install this release to the same install location as release 8.0 or above, the product in the current location is moved to a backup directory name.

For example, if the 7.0 product is installed in the default install location, `/opt/microfocus/VisualCOBOL`, during the installation process it is moved to `/opt/microfocus/VisualCOBOL.BKP.YYYY-MM-DD.HH:MM:SS`. The new release will be installed in `/opt/microfocus/VisualCOBOL`. The backup location will store your original installation along with any files you deployed to that directory. It will also contain any configuration files you modified post-install.

When installing 9.0 and above the installer moves a number of specific configuration files to a different configuration location and symbolically links them back to the new release install location. The configuration location will be one of the following:

- The default `config` location is `/opt/microfocus/config/`.
- For non-root installation, the default location is `$HOME/microfocus/config/`.
- To specify your own configuration location, run the setup file with the following command-line option: `-mfconfiglocation=[location]`

The setup file creates a directory in the configuration location using a 5-digit checksum of the `$COBDIR` path. This is so that each configuration location is unique to each product installation. The configuration files and directories are then placed in this `COBDIR` checksum directory. In the following example, the install location generates a checksum of 39082.

The file `/opt/microfocus/config/39082/COBDIRlocation.txt` details the `COBDIR` the configuration area is associated with.

If you have changed any other files in the original installation, you need to be copy these manually from the backup directory, /opt/microfocus/VisualCOBOL.BKP.YYYY-MM-DD.HH:MM:SS, into the install location after the upgrade installation is complete.

You can access the configuration area from \$COBDIR/etc/config.

Currently, the setup file only moves the following files and directories, where applicable:

Source	Destination
\$COBDIR/etc/mfds	/opt/microfocus/config/39082/mfds/mfds
\$COBDIR/etc/ccsid	/opt/microfocus/config/39082/config/ccsid
\$COBDIR/etc/secrets	/opt/microfocus/config/39082/secrets
\$COBDIR/bin/mf370ctl.cfg	/opt/microfocus/config/39082/config/mf370ctl.cfg
\$COBDIR/bin/CCI.INI	/opt/microfocus/config/39082/config/CCI.INI
\$COBDIR/deploy/.mfdeploy	/opt/microfocus/config/39082/deploy/.mfdeploy
\$COBDIR/etc/cas/CTFesjcl.cfg	/opt/microfocus/config/39082/cas/CTFesjcl.cfg
\$COBDIR/etc/cas/dfhdrdat	/opt/microfocus/config/39082/cas/dfhdrdat
\$COBDIR/etc/commonwebadmin.json	/opt/microfocus/config/39082/escwa/commonwebadmin.json
\$COBDIR/etc/mfdsacfg.xml	/opt/microfocus/config/39082/mfds/mfdsacfg.xml
\$COBDIR/etc/mfdsacfg.dat	/opt/microfocus/config/39082/mfds/mfdsacfg.dat
\$COBDIR/etc/mf-client.dat	/opt/microfocus/config/39082/mfds/mf-client.dat
\$COBDIR/etc/mf-server.dat	/opt/microfocus/config/39082/mfds/mf-server.dat
\$COBDIR/etc/cobol.dir	/opt/microfocus/config/39082/config/cobol.dir
\$COBDIR/etc/cobopt	/opt/microfocus/config/39082/config/cobopt
\$COBDIR/etc/cobopt64	/opt/microfocus/config/39082/config/cobopt64
\$COBDIR/etc/cobjvm.cfg	/opt/microfocus/config/39082/config/cobjvm.cfg
\$COBDIR/etc/cobutf8.cfg	/opt/microfocus/config/39082/config/cobutf8.cfg

Source	Destination
\$COBDIR/etc/default.tcf	/opt/microfocus/config/39082/config/default.tcf
\$COBDIR/etc/mfescache.cfg	/opt/microfocus/config/39082/config/mfescache.cfg
\$COBDIR/etc/dsdef.cfg	/opt/microfocus/config/39082/config/dsdef.cfg

Licensing Coexistence when Upgrading to Release 10.0

With release 10.0 of the Visual COBOL product suite, the SafeNet Sentinel licensing technology has been deprecated. This can result in some compatibility issues if you install 10.0 on a machine where there are other Micro Focus products or versions installed that use SafeNet Sentinel licensing. While the 10.0 installation process has been designed to address such issues, you should be aware of the following scenarios and if any action might be required to ensure licensing works as expected:

Scenarios

Your installed products use SafeNet Sentinel Licenses (Windows and UNIX)



Warning: Installing 10.0 deprecates SafeNet Sentinel licensing on the machine.

If you use SafeNet Sentinel licenses for any other Micro Focus products, such as Enterprise Analyser or Relativity, you need to contact your account manager to obtain AutoPass licenses for these products. See the *Troubleshooting* section further in this topic, *Action 7* for how to obtain a list of your installed licenses.

Your older products use AutoPass licenses (Windows and UNIX)

Existing AutoPass licenses are compatible with the 10.0 products.

Upgrading to 10.0 (UNIX)

After installing 10.0 on a machine with a previous version of licensing installed, the lserv daemon is retained (and might be running) but is not required. See *Troubleshooting > Action 2* for details.

Downgrading from 10.0 (Windows and UNIX)

In order to revert to a previous version of the product (for example, if 10.0 is installed but no longer required), the 10.0 product and licensing must be uninstalled. See *Troubleshooting > Action 1* for details.

Installing a product or Patch Update of an older product release (UNIX)

Use the "skip license installation" command line arguments.

- See *Troubleshooting > Action 3* for details.
- Else, see *Troubleshooting > Action 4* to reset mfcesd.
- SystemD may be overwritten - see *Troubleshooting > Action 6*.

Installing a product or Patch Update of an older product release (AIX only)

If after 10.0 is installed a customer installs a Patch Update for an older release, the lserv entry is moved back to /etc/inittab.

- See *Troubleshooting > Action 3* about how to avoid this.
- To correct the /etc/inittab entry, see *Troubleshooting > Action 5*.
- Alternatively, re-run the 10.0 license install. See *Troubleshooting > Action 6*.

Troubleshooting

Action 1 To reset licensing from the 10.0 installation to an older product configuration, you need to perform the following:

Windows Uninstall the product and the License Manager from "Uninstall a Program" in the Windows Control Panel.

UNIX Execute the following commands:

```
sudo $COBDIR/bin/Uninstall_[Product Name]_10.0.sh.  
sudo /opt/microfocus/licensing/bin/  
UnInstallMFLicenseServer.sh
```

Action 2 (UNIX) To disable the lserv daemon on a machine, execute the following commands:

```
cd /var/microfocuslicensing/bin  
sudo ./stopmfcesd.sh  
sudo systemctl stop MFSafeNet  
sudo systemctl disable MFSafeNet
```

Action 3 When installing an older release or Patch Update, use `-skipsafenet -skipautopass` to the install command. This will skip the licensing installation for that release.

Action 4 To restart mfcesd from the correct location, execute the following commands:

```
cd /var/microfocuslicensing/bin  
sudo ./stopmfcesd.sh  
cd /opt/microfocus/licensing/bin  
sudo ./startmfcesd.sh
```

Action 5 To reset the inittab on AIX 7.3/7.4:

1. Edit the `/etc/inittab` file.
2. Delete the line:

```
mFls:2345:wait:sh /var/microfocuslicensing/bin/startlserv.sh 2>&1
```

Action 6 To reinstall the 10.0 licensing and reset any issues from installing a previous version, execute the following:

```
cd [10.0-COBDIR-location]/licensing  
sudo MFLicenseServerInstall.sh force
```

Action 7 In order to get a list of the installed licenses:

Windows

1. From a COBOL command environment, execute `mfsupportinfo`.
2. View the **Micro Focus Licensing** section.

UNIX

1. In a terminal, run `cobsetenv` to set the product environment.
2. Run `mfsupport`.
3. See `mfpoll.txt` for the licenses details.

Micro Focus Visual COBOL Development Hub Installation Options

Installing into a different location

To install in a different location use the `-installlocation="Location"` parameter to specify an alternative directory location. For example:

```
./setup_visualcobol_devhub_10.0_platform -installlocation="full path of new location"
```



Note: You can use variables when specifying an absolute path for `-installlocation`. For example, the following examples are equivalent:

```
-installlocation="/home/myid/installdir"
```

```
-installlocation="$HOME/installdir"
```

You can see details about which additional parameters can be passed to the install script if you enter the `-help` option.

Configuring the Enterprise Server installation

You can use the following options to configure the Enterprise Server installation: [`-ESsysLog="Y/N"`] [`-ESadminID="User ID"`] [`-CASrtDir="location"`], where:

- ESsysLog** Use this to enable ("Y") or disable ("N") Enterprise Server system logging. Logging is enabled by default. Log files are saved in `/var/mfcobol/logs`.
- ESadminID** Sets the Enterprise Server System Administrator Process User ID from the command line - for example, `-ESadminID="esadm"`. The default user ID is the one that runs the installer.
- CASrtDir** Specifies the location where the Enterprise Server run-time system files are placed - for example, `-CASrtDir="/home/esuser/casrt/es"`. The default location is `/var/mfcobol/es`.

Installing Silently

You can install Micro Focus products silently by using command line parameters to specify the installation directory, user information, and which features to install. You must execute the command with superuser permissions.

You can use the following command line arguments to install silently on UNIX/Linux. You need to execute the commands as root:

```
-silent -IacceptEULA
```

For example, execute:

```
setup_filename -silent -IacceptEULA
```

Installing using the TMPDIR environment variable

By default, the product installer uses `/tmp` for temporary files and log files during installation. If `/tmp` is not available on your system you can set the environment variable `TMPDIR` to an alternative location:

```
TMPDIR=/home/user/tmp  
Export TMPDIR
```

Then run the installation as normal.



Note:

The TMPDIR setting is lost when the installer is elevated to root user within the installer. This occurs when you run the installer as a non-root user, and are prompted for the root password during the installation process. Micro Focus recommends that you log in as root, set TMPDIR and then run the installer. If you use sudo to run the installer, then use the following command-line syntax:

```
sudo TMPDIR=$TMPDIR setup...
```

or:

```
sudo TMPDIR=/home/user/tmp setup...
```

Installing Without Superuser Credentials

Micro Focus recommends that you install this product with superuser permissions. If, however, you need to perform a non-root installation, check the information below. The setup file supports installing into non-root owned directories.

Licensing considerations

- Multiple users - on a machine that has multiple user accounts that need access to the product and licensing, you must install the product under a user ID that grants read, write, and execution permissions to all users.

By default, most user account areas can only be accessed by the owner. In order for all of the users to be able to use the product and License Manager, the installation must be in an account whose \$HOME directory can be accessed by all other users.

Performing a non-root installation

1. Give execute permissions to the setup file:

```
chmod +x setup_visualcobol_devhub_10.0_platform
```

2. Run the installer with the `-noroot` command line argument:

```
setup_visualcobol_devhub_10.0_platform -noroot
```

This installs the product in the default location, `$HOME/microfocus/VisualCOBOL`, where `$HOME` should point to the top-level login directory for the current user.

The product configuration files are stored in `$HOME/microfocus/config`, and the CAS regions are stored in `$HOME/microfocus/es`, by default.

After installing

Once the installation is complete, you need to run the `cobsetenv` script in order to set up your COBOL environment. To do this, execute the following command:

```
. $HOME/microfocus/VisualCOBOL/bin/cobsetenv
```

In addition, on clean machines where licensing has not been installed before, or has not been installed as the root user, you must set the `MFCES_INIT_LOCATION` environment variable. By default, `MFCES_INIT_LOCATION` is set in `cobsetenv` within the installed product. You must also set it in any scripts which use the COBOL product or set the environment as follows:

```
MFCES_INIT_LOCATION=$HOME/microfocus/licensing/ces/bin/ces.ini  
export MFCES_INIT_LOCATION
```

This provides the location of the `ces.ini` licensing configuration file in the non-root installation area for the COBOL Run-Time System.

You do not need to set `MFCES_INIT_LOCATION` on machines where licensing has been installed using the root user. On such machines, there are files in `/opt/microfocus/licensing/bin` and `mfcasd`, and the Autopass process is running as root. In this scenario, `MFCES_INIT_LOCATION` is commented out

in `cobsetenv` and you do not need to update any of your scripts with the `MFCES_INIT_LOCATION` settings. The product installed in a non-root location uses the root install licensing.

Configuring ports

The `/etc/services` file for the registration of port 86 is owned by the root user and cannot be changed without superuser permissions.

You need to ensure that this file includes the `mfcobol` port entries. On most new operating systems, the entries are present.

However, on some operating systems these port entries might be missing. The setup file reports this issue before installing the product. To resolve it, you need to edit `/etc/services` manually in a text editor with root permissions and add the following two lines:

```
mfcobol      86/tcp      # Micro Focus Cobol
mfcobol      86/udp      # Micro Focus Cobol
```

Additional arguments

Specify `-ESadminID="username"`, if you want to use the SOA functionality. When using the `-noroot` command-line option, the value of the `-ESadminID` username must be the current user ID you are running the installer as or the installer gives errors when updating the file permissions. If you need CAS and any other associated tools to run as a specific user, then you need to run the non-root installation as that user.

For non-default installation locations for the product and the product configuration files, use the `-installlocation`, `-mfconfiglocation`, and `-CASrtDIR` command line arguments. See *Installation Options* for details.

AutoPass service configuration

Installing the product without Superuser credentials does not create the required AutoPass service configuration file - `MFAutoPass.service`. A user with Superuser privileges must create this file (and the one detailed in *MFCESD service configuration*) in `/usr/lib/systemd/system`, and then start the service before anyone can license and use the product.


```
[Unit]
Description=Micro Focus AutoPass Licensing Daemons.
Documentation=http://supportline.microfocus.com

[Service]
Type=forking
ExecStart=<HOME>/microfocus/licensing/autopass/autopassdaemon.sh start
ExecStop=<HOME>/microfocus/licensing/autopass/autopassdaemon.sh stop

Restart=no

[Install]
WantedBy=multi-user.target
```

where `<HOME>` is the path to the home directory for the user that installed the product.

 **Important:** Any users required to license and use the product must have access to this home directory.

Once the configuration file has been created, the service can be managed, with Superuser privileges, using the following commands:

```
systemctl reenabte MFAutoPass  *> enables the service
systemctl start MFAutoPass     *> starts the service
systemctl status MFAutoPass    *> checks the service status
```

MFCESD service configuration


Installing the product without Superuser credentials does not create the required MFCESD service configuration file - `MFCESD.service`. A user with Superuser privileges must create this file (and the one detailed in *AutoPass service configuration*) in `/usr/lib/systemd/system`, and then start the service before anyone can license and use the product.

```
[Unit]
Description=Micro Focus AutoPass Licensing Daemons.
Documentation=http://supportline.microfocus.com
After=network-online.target
Wants=network-online.target

[Service]
Type=forking
ExecStart=<HOME>/microfocus/licensing/ces/bin/startmfcesd.sh
ExecStop=<HOME>/microfocus/licensing/ces/bin/stopmfcesd.sh
Restart=no

[Install]
WantedBy=multi-user.target
```

where `<HOME>` is the path to the home directory for the user that installed the product.

 **Important:** Any users required to license and use the product must have access to this home directory.

Once the configuration file has been created, the service can be managed, with Superuser privileges, using the following commands:


```
systemctl reenabte MFCESD  *> enables the service
systemctl start MFCESD    *> starts the service
systemctl status MFCESD   *> checks the service status
```

After Installing

- Check the *Product Documentation* section of the [OpenText Support and Services Documentation Web site for Micro Focus products](#) for any documentation updates.

Setting up the product

If you have installed the product to a directory other than the default one, you need to set the environment as described below.


 **Note:** The default directory is `/opt/microfocus/VisualCOBOL`.

1. To set up your product, execute:

```
. <product-install-dir>/bin/cobsetenv
```

2. To verify that your product is installed, execute:

```
cob -V
```

 **Important:** These commands set the environment only for the current shell. You need to execute them for each new shell that you start.

To avoid having to run `cobsetenv` for every shell, add these commands to the shell initialization files (such as `/etc/profile`, `/etc/bashrc`).

Note that `cobsetenv` is only compatible with POSIX-like shells, such as `bash`, `ksh`, or `XPG4 sh`. It is not compatible with C-shell or pre-XPG4 Bourne shell.



Note: If there are two or more products installed on the machine or the products are installed in non-default locations then the `/opt/microfocus/logs/MicroFocusProductRegistry.dat` data file can be used to find the product locations.

The file contains the following entries:

```
[ Install Location ]#[ Date of Installation ]#[ Product Name ]
```

For example:

```
/home/user1/VisCobol30#2017-01-20#Micro Focus Visual COBOL Development Hub  
3.0  
  
/home/user1/CobolServer30#2017-01-20#Micro Focus COBOL Server 3.0
```

Configuring licensing for older products

If you use release 10.0 and previous releases on the same machine, you need to set the environment variable `MFCES_INIT_LOCATION` to `/opt/microfocus/licensing/bin/ces.ini` in order for licensing to work for the older products. Also, see *Advanced Installation Tasks > Licensing Coexistence when Upgrading to Release 10.0* in the *Installation* section.

Enterprise Server Security Considerations

Starting with this release, the Enterprise Server security functionality provided by the VSAM External Security Manager (VSAM ESM) module is enabled by default out of the box. This means you now need to supply valid credentials when you interact with:

- Enterprise Server Common Web Administration (ESCWA)
- The Micro Focus Directory Server (MFDS)
- enterprise server regions via:
 - ESCWA
 - Certain command-line utilities (such as `casstart`)
 - The Server Explorer window in the new Data Tools available in 10.0
 - IMTK deployment

For more information about the default VSAM Security Manager, see *VSAM ESM Module* in your product Help.

Upgrading an Existing Security Configuration

If security is already configured for a domain (Data Tools, MFDS, or the default Enterprise Server security), the installation process does not change this configuration. If data already exists in either the old or new VSAM ESM default data directory, it will not be altered. However, Micro Focus recommends backing up the following before reinstalling or updating the product - the Data Tools and MFDS configuration files (`commonwebadmin.json` and `mfdsacfg.xml`), the MFDS repository data, and the VSAM ESM Module security data. By default, the MFDS repository data and the VSAM ESM Module data are located under `%ProgramData%\Micro Focus (Windows)` or `$COBDIR/etc` (UNIX).

Default Generated Password for SYSAD

The installation generates a random password for the system administrator account, SYSAD. To retrieve this password, execute the following from an Visual COBOL command prompt or Visual COBOL command prompt (Windows) or from a terminal that has the COBOL environment set (UNIX):

```
mfsecretsadmin read microfocus/temp/admin
```

The password value stored in this vault location is not used by the default Security Manager (VSAM ESM) to validate input credentials. Its purpose is to enable users to initially discover their randomly generated password. Additionally, Server Explorer uses this location to pre-populate the **Micro Focus Servers** connection and the credentials dialog box at region start-up. Once entered, you can optionally save the

credentials in IDE-specific storage. Micro Focus recommends that once the credentials are safely known or changed that you remove this value from the vault (using `mfsecretsadmin delete microfocus/temp/admin`).

Change the Default Password for SYSAD

Micro Focus recommends that you promptly replace this password with one that conforms to your security policy. You can do this from the ESCWA logon page - click **Change Password**. Alternatively, you can use the `esfadmin SETPASSWORD` command and specifying the "vsam_esm" module file.

Authentication in the Browser-Based ESCWA

You need to provide credentials to access ESCWA. After the installation, the ESCWA logon page shows information on how to obtain the default admin (SYSAD) generated password. You can disable this message in the ESCWA Security Settings dialog ("Show Default Security Warning on Log On").

For local installations, the default Directory Server will automatically be authenticated with the ESCWA credentials. Otherwise, you might need to provide its own credentials. You may use the same credentials as the ones for ESCWA.

Note the default 5-minute (300 second) session time out setting for inactivity in ESCWA. If required, you can change this from the ESCWA Security Settings dialog ("Session Inactivity Timeout").

Authentication Inside the Data Tools Utility

The Server Explorer window in Data Tools, requires credentials for the **Micro Focus Servers** node to connect to the default local ESCWA and the MFDS. Additionally, you need to provide credentials to start any regions. By default, the credentials will be pre-populated in the dialog using the values stored in the `microfocus/temp/admin` vault location. These credentials can optionally be stored by the IDE so they do not need to be manually input again.



Note: If you delete the SYSAD user or change the password generated for it by the installer in the default VSAM Security Manager, you need to provide new sufficiently authorized credentials for the Server Explorer connection.

Fileshare

If you want to view or delete Fileshare instances in ESCWA, you now need to log on using authorized credentials (such as the default SYSAD user).

Command-Line Utilities

There are multiple command line utilities that control and access enterprise server region. These use Enterprise Server credentials specified as parameters - for example, `casstart /z`.

See *Administration and Configuration Commands* in your product Help for individual commands to determine how to specify authorized credentials.

Samples and Tutorials

There are a variety of samples and tutorials supplied with the product. Many of these assume that security is not enabled, so to work through these unaltered default security will first need to be disabled. See *To Disable the Default Enterprise Server Security Configuration* in your product Help. If security is not disabled, you will need to take it into account when you:


- Use ESCWA
- Start a region
- Run a cas command line utility

Micro Focus Common Client

The `mf-client.dat` file which is used by the Micro Focus Common Client (MFCC), is configured out-of-the-box to use the default generated "readonly" credentials from the `microfocus/common/readonly` vault location. This means that access to the Micro Focus Directory Server using the default security configuration works automatically for read-only access.

MFCC is used by COBOL web service proxy programs, the Interface Mapping Toolkit service-deployment mechanism, Fileshare clients (when configured appropriately), various utilities such as `cassub` (depending on the operating mode), the CICS Web Interface and CICS Web Services, and product components such as MFCS and ESCWA. See *Micro Focus Common Client* in your product Help.

Configuring the Remote System Explorer Support


 **Note:** The following only applies if you are using Micro Focus Visual COBOL Development Hub with Visual COBOL for Eclipse.

The remote development support from the Eclipse IDE relies upon Micro Focus Visual COBOL Development Hub running on the UNIX machine and handling all requests from the IDE for building and debugging programs. Micro Focus Visual COBOL Development Hub provides a UNIX daemon, the Remote Development Option (RDO) daemon, which initiates the RDO as Eclipse clients connect to it. Whichever environment is used to start the RDO daemon will be inherited for all servers and hence all build and debug sessions.

Configuring the Environment


You may need to configure some aspects of the environment before you start the daemon. This is because when a build or debug session is initiated on the Development Hub from one of the Eclipse clients, the environment used will be inherited from whatever was used to start the daemon. A typical example of the kind of environment that might need to be set up would include database locations and settings for SQL access at build/run time.

Starting the Daemon

 **Important:** Before starting the daemon you must have the following on your UNIX machine:

- A version of Perl.
- A version of Java 8 or later.
- The `as` (assembler) and `ld` (linking) programs on the path, as specified by the `PATH` environment variable.

The daemon can be run with or without parameters. If no parameters are specified, the process relies on the default values in `COBDIR/remotedev/rdo.cfg`.

 **Important:** If Micro Focus Visual COBOL Development Hub has been installed without superuser credentials (see *Installing Without Superuser Credentials*), you must ensure that the following commands are carried out using superuser credentials. This is because the *Micro Focus Dev Hub RSE* and *Micro Focus Dev Hub using SAMBA, NFS, etc* connection types require elevated privileges to authenticate upon connection to the server.

Use the following syntax to start the daemon on the remote host:

```
COBDIR/remotedev/startrdodaemon [<port> <low port>--<high port>]
```

where:

- *<port>* is the port number that the daemon should use to listen for connections from Eclipse. If no value is given, it will default to the value specified in `COBDIR/remotedev/rdo.cfg`; the default value on installation is 4075.

Example: To start the daemon listening on port 4999:

```
$COBDIR/remotedev/startrdodaemon 4999
```

This command will override the default port in `rdo.cfg`.

- `<low port>-<high port>` is the range of ports on which the servers (launched by the daemon) should use to communicate with Eclipse on the client machine. If no values are given, the range defaults to that specified in `$COBDIR/remotedev/rdo.cfg`; the default range on installation is 10000-10003.

Example: To instruct the daemon (on port 4999) to instantiate servers using a range of ports 4090-4993:

```
$COBDIR/remotedev/startrdodaemon 4999 4090-4993
```

This command will also override the default ports in `rdo.cfg`.

If the server has an active firewall, it is important that these ports are open in the firewall settings. You can use the `configrdo` utility to set the default ports in `rdo.cfg` to ones already open in the firewall. If you are running on Red Hat 7.2 (or later) or CentOS 7.2 (or later), you can also use the utility to open the required ports in the active firewall. See *Configuring the firewall* for more information.

Stopping the Daemon

To stop the daemon, type the following command with super-user authority:

```
$COBDIR/remotedev/stoprdodaemon <port>
```

Configuring the firewall

If the server on which Micro Focus Visual COBOL Development Hub is installed is running a firewall, you must ensure that certain ports and services are allowed through so that Eclipse running on a client machine can communicate with it.

To ensure successful communication between the IDE and Micro Focus Visual COBOL Development Hub when a firewall is active, use the `configrdo` utility after initial setup or if you experience problems establishing a connection between the two.



Tip: If you run the client-side and/or server-side connection diagnosis tools, these include a number of tests relating to firewall configuration, and can indicate any problems with the current firewall settings.

Use `configrdo` to configure the following settings:

- Set the default RDO daemon and server ports used by Micro Focus Visual COBOL Development Hub.
- Open additional ports in the firewall.

This option is only available on the following platforms: Red Hat 7.2 and later, or CentOS 7.2 and later.

- Add the `ssh` and `samba` services to the firewall.

This option is only available on the following platforms: Red Hat 7.2 and later, or CentOS 7.2 and later.

These changes can be temporary (for the duration of the current firewall being active), or be made permanent (so that they persist after a system reboot). If you are not running any of the supported platforms listed above, use your operating system's firewall commands to perform the equivalent functions.

To configure the firewall settings

To be able to run this utility:

- You must have super-user authority (e.g. root user)
- `$COBDIR` must be set to the value of the product install folder for Micro Focus Visual COBOL Development Hub.

1. From a shell command, run the following:

```
$COBDIR/remotedev/configrdo
```

2. At the `Daemon port` prompt, enter the port number that the daemon should listen on, or press **Enter** to accept the default.



Note: The default settings for these port prompts are specified in the `rdo.cfg` configuration file.

The `Server range` is a range of port numbers that a required RDO server will be started on when the daemon receives a request.

3. At the `Server range low port` prompt, enter the starting number of the server port range and press **Enter**, or press **Enter** to accept the default.
4. At the `Server range high port` prompt, enter the ending number of the server port range and press **Enter**, or press **Enter** to accept the default.

The defaults are written to the `rdo.cfg` configuration file.

If you are running this utility on Red Hat 7.2 (or later) or CentOS 7.2 (or later), an additional prompt is displayed; otherwise, the utility closes.

5. At the `Do you want to configure the firewall` prompt, press **Y** and then **Enter** to configure further firewall settings, or press **N** and then **Enter** to close the utility. If you selected **Y**, the configured firewall zones are listed.
6. To configure an existing zone, press the corresponding number and then **Enter**, or press **Enter** for the default zone (as indicated at the end of the prompt).



Note: At this point, you can also create a new zone: press **N** and then **Enter**, and then type the new zone name and press **Enter**. The new zone is listed, and you can now select its corresponding number to configure it.

The current firewall status is displayed, where it checks if the currently specified ports are open in the firewall; if they are not, the utility adds them to the firewall settings.

7. If you need to open more ports, press **Y** and then **Enter**, and then enter either a single port number, or a range, and then press **Enter**.

The additional ports are opened.

8. If either of the `ssh` and `samba` services are not running in the firewall zone, you are prompted to add them: press **Y** and then **Enter** or **N** and then **Enter**, as appropriate, for each service.



Note: If the service is already running, you are not prompted.

An overview of the firewall settings is displayed.

9. To save the changes permanently (that is, even after the firewall is restarted), press **Y** and then **Enter**; to save the settings for the firewall until it is next stopped, **N** and then **Enter**.

The utility is closed.



Note: If you need to remove any ports or services you have added to the firewall, use the `firewall-cmd` utility that is part of the operating system.

Enabling SHIFT-JIS

By default, support for the character encoding for the Japanese language, Shift-JIS, is not available on Ubuntu and on RedHat OS version 8 or later.

You need to generate the Shift JIS locale on your machine to be able to execute Shift-JIS applications on these platforms. You can do this as follows:

1. On RedHat 8, ensure that the `glibc-locale-source` package is installed.

2. Execute the following command with superuser rights in order to generate a Shift-JIS locale using the charset:

```
sudo localedef -f SHIFT_JIS -i ja_JP ja_JP.sjis
```

3. Set the COBUTF8 environment variable to the generated Shift-SJIS locale and LANG to a UTF8 locale:

```
export COBUTF8=ja_JP.sjis  
export LANG=ja_JP.UTF-8
```

4. Run the cobutf8 utility:

```
cobutf8 <command>
```

See your product documentation for more details about cobutf8.

Repairing on UNIX

If a file in the installation of the product becomes corrupt, or is missing, we recommend that you reinstall the product.

Before performing a repair of the installation, Micro Focus recommends that you create backups of any configuration files of the product that you might have changed.

Uninstalling

Before you uninstall the product, ensure that the Enterprise Server Common Web Administration (ESCWA), the Micro Focus Directory Server, and any enterprise server regions are stopped.

To uninstall this product:

1. Execute as root the `Uninstall_VisualCOBOLDevelopmentHub10.0.sh` script in the `COBDIR/bin` directory.



Note: The installer creates separate installations for the product and for Micro Focus License Administration. Uninstalling the product does not automatically uninstall the Micro Focus License Administration or the prerequisite software. To completely remove the product you must uninstall the Micro Focus License Administration as well.

To uninstall Micro Focus License Administration:

1. Execute as root the `UnInstallMFLicenseServer.sh` script in the `/opt/microfocus/licensing/bin` directory.

The script does not remove some of the files as they contain certain system settings or licenses.

You can optionally remove the prerequisite software. For instructions, check the documentation of the respective software vendor.

Licensing Information



Note:

- The SafeNet Sentinel licensing system has been deprecated. This product uses the Micro Focus AutoPass licensing technology. Contact your account manager to replace your existing SafeNet Sentinel with AutoPass licenses. Also, see *Advanced Installation Tasks > Licensing Coexistence when Upgrading to Release 10.0* in the *Installation* section in your product Help.
- If you have purchased AutoPass licenses for a previous release of this product, those licenses will also enable you to use this release.
- If you are unsure of what your license entitlement is or if you wish to purchase additional licenses, contact your sales representative or [OpenText Support for Micro Focus Products](#).

To start Micro Focus License Administration

Log on as root, and from a command prompt type:

```
/opt/microfocus/licensing/bin/cesadmintool.sh
```

Configuring licensing for older products

If you use release 10.0 and previous releases on the same machine, you need to set the environment variable `MFCES_INIT_LOCATION` to `/opt/microfocus/licensing/bin/ces.ini` in order for licensing to work for the older products. Also, see *Advanced Installation Tasks > Licensing Coexistence when Upgrading to Release 10.0* in the *Installation* section.

Installing licenses

You need a license file (with an `.xml` extension for AutoPass licenses). You need to install AutoPass licenses into the existing Micro Focus License Administration tool, and not in the AutoPass License Server.

Applying your license file

1. Start the Micro Focus License Administration tool and select the **Manual License Installation** option by entering 4.
2. Enter the name and location of the license file.

To obtain more licenses

If you are unsure of what your license entitlement is or if you wish to purchase additional licenses for Visual COBOL, contact your sales representative or OpenText Support for Micro Focus Products.

Updates and OpenText Support for Micro Focus Products

Our Web site provides up-to-date information of contact numbers and addresses.

Further Information and OpenText Support for Micro Focus Products

Additional technical information or advice is available from several sources.

The product support pages contain a considerable amount of additional information, such as:

- Product Updates on [Software Licenses and Downloads](#), where you can download fixes and documentation updates.
 1. Log into the Software Licenses and Downloads (SLD) site at <https://sld.microfocus.com/mysoftware/download/downloadCenter>.
 2. Select your account and click **Entitlements**.
 3. Search for the product by using any of the available search parameters.
 4. Click **Show all entitlements**.
 5. Click **Get Software** in the Action column for the product you want to download or update.

In the **File Type** column, you see entries for "Software" for any GA products, and "Patch" for any patch updates.
 6. Click **Download** on the relevant row.
- The *Examples and Utilities* section of the OpenText Support for Micro Focus Products Web site, including demos and additional product documentation. Go to <https://supportline.microfocus.com/examplesandutilities/index.aspx>.
- The *Support Resources* section of the OpenText Support for Micro Focus Products Web site, that includes troubleshooting guides and information about how to raise an incident. Go to <https://supportline.microfocus.com/supportresources.aspx>

To connect, enter <https://www.microfocus.com/en-us/home/> in your browser to go to the Micro Focus home page, then click **Support & Services > Support**. Type or select the product you require from the product selection dropdown, and then click **Support Portal**.



Note: Some information may be available only to customers who have maintenance agreements.

If you obtained this product directly from Micro Focus, contact us as described on the Micro Focus Web site for Micro Focus products, <https://www.microfocus.com/support-and-services/contact-support/>. If you obtained the product from another source, such as an authorized distributor, contact them for help first. If they are unable to help, contact us.

Also, visit:

- The Micro Focus Community Web site, where you can browse the Knowledge Base, read articles and blogs, find demonstration programs and examples, and discuss this product with other users and Micro Focus specialists. See <https://community.microfocus.com>.
- The Micro Focus YouTube channel for videos related to your Micro Focus product. See [OpenText YouTube Channel for Micro Focus Products](#).
- Micro Focus webinars: <https://www.microfocus.com/en-us/resource-center/webinar>.

Information We Need

If your purpose in contacting Micro Focus is to raise a support issue with OpenText Support for Micro Focus Products, you should collect some basic information before you contact us, and be ready to share it when you do.

Creating Debug Files

If you encounter an error when compiling a program that requires you to contact OpenText Support for Micro Focus Products, your support representative might request that you provide additional debug files (as well as source and data files) to help us determine the cause of the problem. If so, they will advise you how to create them.

Copyright and Disclaimer

© Copyright 2024 Micro Focus or one of its affiliates.

The only warranties for this product and any associated updates or services are those that may be described in express warranty statements accompanying the product or in an applicable license agreement you have entered into. Nothing in this document should be construed as creating any warranty for a product, updates, or services. The information contained in this document is subject to change without notice and is provided "AS IS" without any express or implied warranties or conditions. Micro Focus shall not be liable for any technical or other errors or omissions in this document. Please see the product's applicable end user license agreement for details regarding the license terms and conditions, warranties, and limitations of liability.

Any links to third-party Web sites take you outside Micro Focus Web sites, and Micro Focus has no control over and is not responsible for information on third-party sites.