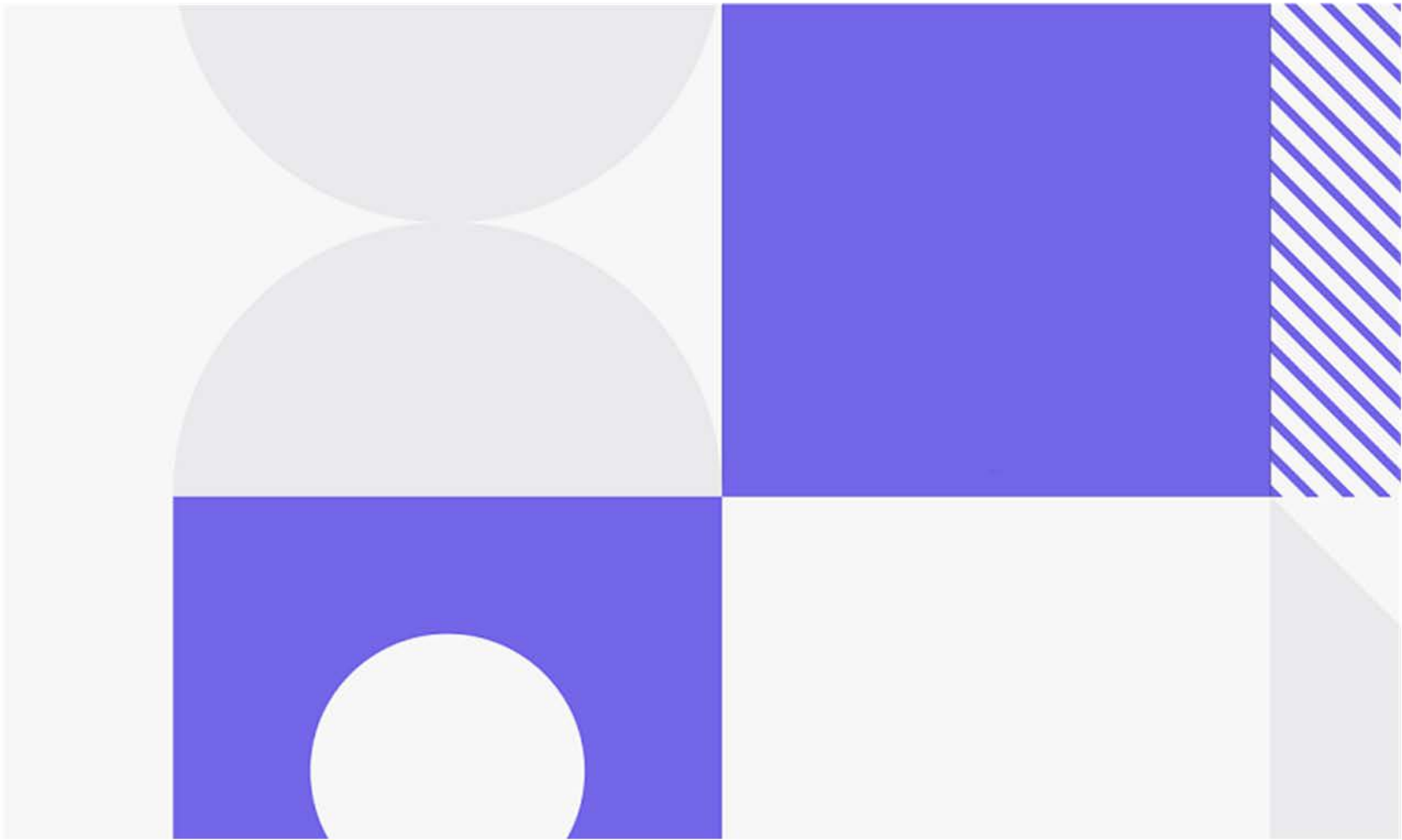
opentext™

Dimensions RM

Software version: 12.11.2 (23.4)

Installation Guide



Product version: 12.11.2 (23.4)

Last updated: October 21, 2023

Table of Contents

Preface

Objective

The purpose of this manual is to describe how to install Dimensions RM, a comprehensive requirements management application that lets development teams capture, engineer, and manage requirements through the entire product life cycle.

Edition Status

The information in this guide applies to *Release 12.11.2 (23.4)* of Dimensions RM. This edition supersedes earlier editions of this manual.

Please note that this release includes the re-branding of Dimensions RM as it moves from Micro Focus to Open Text.

Audience

This manual is primarily intended for system administrators who are responsible for installing Dimensions RM. It presumes that you have knowledge of the operating systems to which you are installing.

Typographical Conventions

The following typographical conventions are used in the online manuals and online help. These typographical conventions are used to assist you when using the documentation; they are not meant to contradict or change any standard use of typographical conventions in the various product components or the host operating system.

italics	Introduces new terms that you may not be familiar with and occasionally indicates emphasis.
bold	Emphasizes important information and field names.
UPPERCASE	Indicates keys or key combinations that you can use. For example, press the ENTER key.
`monospace`	Indicates syntax examples, values that you specify, or results that you receive.
`monospaced italics`	Indicates names that are placeholders for values you specify; for example, *`filename`*.

`monospace bold`	Indicates the results of an executed command.
vertical rule |	Separates menus and their associated commands. For example, select File | Copy means to select Copy from the File menu. Also, indicates mutually exclusive choices in a command syntax line.
brackets []	Indicates optional items. For example, in the following statement: `SELECT [DISTINCT], ` DISTINCT is an optional keyword.
. . .	Indicates command arguments that can have more than one value.

Printing Manuals

As part of your Dimensions license agreement, you may print and distribute as many copies of the Dimensions manuals as needed *for your internal use, so long as you maintain all copies in strict confidence and take all reasonable steps necessary to ensure that the manuals are not made available or disclosed to anyone who is not authorized to access Dimensions under your Dimensions license agreement*.

Contacting Technical Support

Micro Focus provides technical support for all registered users of this product, including limited installation support for the first 30 days. If you need support after that time, contact Micro Focus Support at the following URL and follow the instructions:

`http:///supportline.microfocus.com`

Language-specific technical support is available during local business hours. For all other hours, technical support is provided in English.

The Micro Focus Support web page can also be used to:

- Report problems and ask questions.
- Obtain up-to-date technical support information, including that shared by our customers via the Web, automatic e-mail notification, newsgroups, and regional user groups.
- Access a knowledge base, which contains how-to information and allows you to search on keywords for technical bulletins.
- Download fix releases for your Micro Focus products.

License and Copyright Information for Third-Party Software

For license and copyright information of third-party software included in this release, check the file `Third_Party_Licenses.txt`, which can be found in the Dimensions RM installation directory, e.g. C:\Program Files\Open Text\Dimensions 12.11.2 (23.4)\RM.

Chapter 1

Before Installing

Introduction

NOTE Other installation procedures are also discussed or mapped out in this guide, for example:

- Configurations in which your Oracle RDBMS is located on a remote network node.
- Configurations in which an Administrator Oracle client is required.
- Upgrading an existing Dimensions RM server and associated RDBMS (where appropriate).

However, you may want to contact Micro Focus Support for additional advice with more complex installations.

Dimensions RM is a comprehensive requirements management application that lets development teams capture, engineer, and manage requirements through the entire product life cycle.

This guide provides instructions for licensing Dimensions RM, installing and configuring your RDBMS and Administrator Oracle client (where necessary), installing Dimensions RM, and upgrading from previous versions of Dimensions RM, your RDBMS, and Open Text Auto Pass.

The instructions in this guide are *principally* for single-server installations of the Dimensions RM product comprising:

- One of the following database configurations:
  - **Oracle:**
    - Oracle 12c
    - Oracle 18c
    - Oracle 19c
  - **Microsoft SQL Server:**
    - MS SQL Server 2017 with cumulative update 25
    - MS SQL Server 2019
  - **PostgreSQL:**
    - PostgreSQL 14
    - PostgreSQL 13
- A pre-installed Open Text Auto Pass.
- Pre-installed Microsoft Office (32-bit or 64-bit). For details, see chapter "Microsoft Office Requirements" on page 17.
- A Dimensions RM server, providing the following components:
  - Web Server.
  - SyncEngine.
  - ALF Emitter.
  - RM Mail Service.

- RM Web Service.
- RM Admin Clients.

NOTE Other installation procedures are also discussed or mapped out in this guide, for example:

- Configurations in which your Oracle RDBMS is located on a remote network node.
- Configurations in which an Administrator Oracle client is required.
- Upgrading an existing Dimensions RM server and associated RDBMS (where appropriate).

However, you may want to contact Micro Focus Support for additional advice with more complex installations.

System Requirements

IMPORTANT! For the list of currently supported RDBMS platforms, chip architectures, operating-systems, Web servers, Web browsers, and Micro Focus and third-party integrations, see the Dimensions RM Supported Platform Matrix:

https://www.microfocus.com/documentation/dimensions-rm/

The following list includes various requirements and notes not otherwise included on the supported platform Web site:

- **Micro Focus Auto Pass:** Micro Focus Auto Pass must be installed in order to implement a fully licensed release of Dimensions RM, rather than to exercise the 30-day evaluation option. For details, see https://docs.microfocus.com/itom/AutoPass_License_Server:latest/Home.
- **UNIX RDBMS** must be installed on a remote UNIX network node.
- **For Oracle databases:**
  - **Oracle Administration Client:** Depending on your environment, you may need to install a supported 64-bit Administrator Oracle Client. For more information, see chapter "The Administrator Oracle Client" on page 128.
- **For Microsoft SQL Server:**
  - **64-bit ODBC System DSN:** You need to set up a 64-bit ODBC System DSN on SQL Server Native Client 11 driver in order to use the following Dimensions RM components:
    - A Dimensions RM server communicating with a *remote* RDBMS.
    - A Dimensions RM server communicating with a local 64-bit Windows RDBMS.
    - A Dimensions RM Admin Client communicating with a Dimensions RM database, no matter where located.
- **Web Server:**
  - The Web server must be installed on a Windows machine.

  - When using Oracle databases, a 64-bit Oracle Administrator client must be installed on the same machine as the Web server.
  - When using a Microsoft SQL Server database, a 64-bit ODBC System DSN must be configured on the same machine as the Web server.
- **Microsoft Office (32-bit or 64-bit):** Including .NET Programmability Support, must be installed on the Dimensions RM server. For further information, see chapter "Microsoft Office Requirements" on page 17.

Prerequisites for the Dimensions CM to Dimensions RM Integration

For Integration with Dimensions CM, the following prerequisites must be satisfied:

- Both Dimensions CM and Dimensions RM must have been installed and both must be at compatible release levels. See the Micro Focus Integrations page of the relevant RM release: https://www.microfocus.com/documentation/dimensions-rm/.
- A Dimensions CM desktop client must be installed on the Dimensions RM web server machine.
- If you are using Dimensions CM and Dimensions RM against an Oracle RDBMS, you must make sure that they are not sharing the same Oracle instance.
- Before you can begin to establish any of the Dimensions RM to Dimensions CM associations referenced in this or the*Dimensions CM-Dimensions RM ALM Integration Guide*, the `rmcm.xml` configuration file on the Dimensions RM web server machine must be edited to include the URL of the Dimensions CM server, as described below:

  a On the Dimensions RM web server machine, navigate to:

  ```
  <RM-Install-Directory>\conf
  ```

  b Open the following configuration file in a text editor:

  ```
  rmcm.xml
  ```

  This file contains the following lines:

  ```
  <project>
        <!--  CMServer url="http://localhost:8080" -->
        <CMServer url="" />
  </project>
  ```

  c Update the Dimensions CM URL with the correct information for the Dimensions CM server. If Dimensions CM is installed on the same machine as the Dimensions RM web server and was installed with the default port number `8080`, then the commented out URL on the preceding line will be the appropriate URL.
- The following Dimensions RM to Dimensions CM associations must have been established by a Dimensions RM:
  - The requisite Dimensions RM instances to one or multiple Dimensions CM products (see the *Dimensions CM-Dimensions RM ALM Integration Guide*).
  - The requisite Dimensions RM baselines or collections to one or multiple Dimensions CM projects/streams (see *Dimensions CM-Dimensions RM ALM Integration Guide*).

Conversely, to enable Dimensions RM users to look at Dimensions CM requests, after the above steps have been completed, a Dimensions CM user must associate Dimensions RM requirements to Dimensions CM requests.

Upgrade Scenarios

For new installations see chapter "Installing Dimensions RM" on page 51.

There is, strictly speaking, no "upgrade" mechanism for Dimensions RM; the older version must be un-installed before initiating the installation of the 12.11.2 (23.4) release.

Find the scenario below that best matches your needs:

1 **Installing Dimensions RM on the Same Server as the Earlier Release:** The high-level steps, are listed below.

a Dimensions RM release 12.11.2 (23.4) requires Micro Focus Auto Pass release 11.5 or higher to be installed, upgrade AutoPass if using a previous version.

b If the version of RM in use is using the Serena License Manager, upgrade your Auto Pass installation.

IMPORTANT! Serena License Manager (SLM) is no longer supported.

c Review the Upgrade Checklist, followed by associated tasks in Chapter 2, "Upgrading Dimensions RM Server" on page 21.

d Convert / Upgrade all RM Instances.

e Return saved or backed-up files to their proper locations. This includes ANY files modified or created in order to support the execution of Dimensions RM or the forms and templates created to augment its use.

2 **Migrating to a fresh Oracle installation**

a Perform all pre-upgrade (pre-migration) tasks, including backing up the database, all Dimensions RM instances, and un-installing RM.

b If the fresh Oracle installation is on the same server:

- Save TNSames files for both the RDBMS server and the Oracle client.
- Use the Oracle Universal Installer (OUI) to remove your Oracle products following the Oracle documentation.
- Uninstall the Oracle client.
- Reboot the RDBMS server.
- Delete both the root Oracle and program files directories.
- Reboot the RDBMS server again.

c Install and configure the new version of Oracle; include the Oracle 64-bit client, if not included with the Oracle install.

d Install the new release of Dimensions RM.

e Return saved or backed-up files in their proper locations.

f Restore all RM Instances.

IMPORTANT! The Dimensions RM installer asks which version of Oracle it is being installed to and installs files specific to the version of Oracle that you specify.

Planning for the Installation

Dimensions RM is a comprehensive requirements management application that lets development teams capture, engineer, and manage requirements through the entire product life cycle.

This guide provides instructions for:

- Installing and configuring the RDBMS
- Installing and configuring the Administrator Oracle client or MS SQL DSN (where necessary)
- Installing Dimensions RM
- Upgrading from previous versions of Dimensions RM

The following are a series of checklists to be used for planning and preparing your upgrade or installation:

	Installation	Upgrade
Server	"Installing Dimensions RM Server" on page 33	"Upgrading Dimensions RM Server" on page 21
Admin Client	"Installing the Dimensions RM Admin Client" on page 43	"Installing the Administrator Client" on page 45

High-Level Requirements

To help ensure that your installation is a success, review the following installation requirements and tips.

General Requirements

Before you install, make sure that:

- You have worked through the chapter "Planning for the Installation" on page 15.
- The host names of the server computers that will host the database and the licensing tool Micro Focus Auto Pass have been identified. If a single computer is to be used for all software components, it can host both the Dimensions RM server and client.

IMPORTANT!

- Ensure that the AutoPass port (default **5814**) is open for inbound connections on the AutoPass server.
- Ensure that the AutoPass port (default 5814) is open for outbound connections on the RM server.
- Serena License Server (SLM) is no longer supported.

- When operating in an IPv6-only environment, IPv4 must be installed on the server running Dimensions RM. It is not required to enable IPv4 after installing it.
- **Oracle only:** For a Dimensions RM client-only installation (and for various other installation configurations), that the requisite Oracle Administrator client has been installed.

NOTE Oracle only: the Oracle client path must be first in the Windows PATH variable.

- If you will be installing the e-mail notification service, that you know the name of the computer running the service and the name of the SMTP mail server to be used.
- 32-bit or 64-bit edition of Microsoft Office, including .NET Programmability Support must be installed on the Dimensions RM server for support of document export, RM Import and RM Import Designer tools,
  - For supported versions of Microsoft Office please check the support matrix file in the following location: https://www.microfocus.com/documentation/dimensions-rm/
  - For further information, see chapter "Microsoft Office Requirements" on page 17.
- No other applications are running.

When Using Oracle with Dimensions RM

Correctly Configuring the Oracle RDBMS

The Oracle RDBMS instance must be configured correctly before Dimensions RM is installed. Please see "Installing and Configuring Oracle" on page 127.

The following link may be used to check information about software requirements for Oracle installation http://docs.oracle.com/database/121/NTCLI/pre_install.htm#NTCLI1255

When Using Microsoft SQL Server with Dimensions RM

The following requisites have to be met before installing Dimensions RM:

- Microsoft SQL Server is installed
- A database instance to receive the data of Dimensions RM exists
- A configured 64-bit System DSN exists on the application server and Web server.

Please follow the following link to check information about hardware and software requirements for installing MS SQL Server: https://docs.microsoft.com/en-us/sql/sql-server/install/hardware-and-software-requirements-for-installing-sql-server#hwswr

When Using PostgreSQL with Dimensions RM

The following requisites have to be met before installing Dimensions RM:

- PostgreSQL is installed
- A database instance to receive the data of Dimensions RM exists
- A configured 64-bit System DSN exists on the application server and Web server.

IMPORTANT! Dimensions RM supports only one PostgreSQL database instance per database server.

Microsoft Office Requirements

It is **highly recommended** that Microsoft Office is installed on the Dimensions RM server. If Microsoft Office is not installed, Dimensions RM is running with the following limitations:

- If **Microsoft Word** is not installed on the server:
  - DOCX format is not available for export. Documents export to DOC instead.
  - PDF format is not available for export. Documents export to DOC instead.
  - When exporting to Microsoft Word, the Table of Contents shows page 1 for all chapters.
  - Attachments cannot be exported.
  - Import of Word files through RM Browser is not available.
- If **Microsoft Excel** is not installed on the server:
  - XLSX format is not available for export of requirements or documents. Files export to XLS instead.
- If **Microsoft PowerPoint** is not installed on the server:
  - Dashboards cannot be exported to PPTX or PDF format.

If you want to use Microsoft Office on the Dimensions RM server, the following criteria have to be met:

- The 32-bit or 64-bit edition of Microsoft Office, including .NET Programmability Support, must be installed. For supported versions of Microsoft Office please check the support matrix file in the following location: https://www.microfocus.com/documentation/dimensions-rm/
- Microsoft Word, Microsoft Excel, and Microsoft PowerPoint must be installed.

SSO Considerations

Single Sign On is supported in the following scenarios:

- **Open Text Solution Business Manager (SBM)**

  The SBM server installation must be SSO enabled.

- **Open Text Dimensions CM**

  The Dimensions CM server installation must be SSO enabled.

- **Windows SSO**

  There are no prerequisites, but currently Windows SSO is only supported for the Web Browser. The Admin Client tools, Web Services, and RM Import do not support Windows SSO.

  The Windows SSO zip file is no longer included with the Dimensions RM distribution. Please contact support for a copy of this file.

The SBM or Dimensions CM software and documentation can be downloaded from the Micro Focus web site. For information on installing and enabling an SBM or Dimensions CM SSO server, see the *Installation Guide* and *Administrator's Guide* for the relevant product.

CAUTION!

- When installing Dimensions RM with SSO, **specify a host name** rather than an IP address. Otherwise SSO may not work correctly with Web applications. The host name **must be exactly the same** configured for the gatekeeper in SBM or Dimensions CM.
- The Dimensions RM SSO installation changes many configuration files to ensure that SSO performs correctly. It is difficult to perform these configuration changes manually. We recommend that if non-SSO configuration is to be modified to support SSO, you might consider re-installing the product, or check with Micro Focus RM Support for assistance.

IMPORTANT!

- The Micro Focus SSO Server component of Dimensions CM or SBM must be installed to a system that is accessible to the RM server.
- The Micro Focus SSO Server must be fully configured and ready to support CAC, LDAP, or any other authentication method you will be using. See the SBM or Dimensions CM documentation for information on installing and configuring a Micro Focus SSO Server.
- If you install Dimensions RM and CM to the same server and enable SSO in RM, then SSO will also be in enabled in Dimensions CM.

SBM/Dimensions CM Prerequisites

- The Micro Focus SSO Server component of Dimensions CM or SBM must be installed to a system that is accessible to the RM server.
- The Micro Focus SSO Server must be fully configured and ready to support CAC, LDAP, or whatever authentication method you will be using. See the SBM or Dimensions CM documentation for information on installing and configuring a Micro Focus SSO Server.

Prerequisites for SSO Authentication

- **Client Prerequisites**

  The Dimensions RM SSO software is all server side, so there are no client prerequisites.

- **Server Prerequisites**

  The following information is requested by the Dimensions RM installer. This information can be determined by examining the configuration of your SBM or Dimensions CM SSO server.

Name of field in RM installer	Description
Host Name	The host name or IP address of the computer that hosts your Micro Focus Single Sign On server.
SSO	The HTTP (default = 8085) or HTTPS (default = 8243) port used by the SSO server. **NOTE** If the specified port is not an HTTPS port, then the **Secure (HTTPS) Connection** checkbox (see below) *must* remain unchecked.
Secure (HTTPS) Connection	Enable this checkbox if the Micro Focus SSO Server uses Secure Socket Layer (SSL) communication. **NOTE** Changing this checkbox will reset the **SSO** port to the default HTTP or HTTPS port.

Prerequisites for SSO with CAC Reader Authentication

- **Client Prerequisites**

  The following client side prerequisites are required:

  - Installation of Common Access Card (CAC) ActivClient 6.1 or later software. All configuring of the ActivClient client, if necessary, should be performed as described in the vendor documentation. How to log in using CAC and your PIN in the various Dimensions RM clients is described in the Dimensions RM client documentation.
  - Each user has a personal CAC.
  - A CAC Reader is attached to the client machine.

- **Server Prerequisites**

  The following information is requested by the Dimensions RM installer. This information can be determined by examining the configuration of your SBM or Dimensions CM SSO server.

Name of field in RM installer	Description
Host Name	The host name or IP address of the computer that hosts your Micro Focus Single Sign On server.
SSO	The HTTP (default = 8085) or HTTPS (default = 8243) port used by the Micro Focus SSO server. **NOTE** If the specified port is not an HTTPS port, then the **Secure (HTTPS) Connection** checkbox (see below) *must* remain unchecked.
Secure (HTTPS) Connection	Enable this checkbox if the Micro Focus SSO Server uses Secure Socket Layer (SSL) communication. **NOTE** Changing this checkbox will reset the **SSO** port to the default HTTP or HTTPS port.

Chapter 2

Upgrading Dimensions RM Server

Checklist Items Before Upgrading Dimensions RM Server

✓

	Download the Platform Matrix Download the Platform Matrix at https://www.microfocus.com/documentation/dimensions-rm/ Use the platform matrix to ensure support for the following: ■ **Supported Windows Operating System** ■ **Supported Microsoft Office Version** ■ **Supported Web Browser** ■ **Supported databases**; if upgrading the database as well as Dimensions RM, please see associated instructions ■ For **Dimensions CM Integration**: Supported Dimensions CM Client versions
	Named Web Service License If Dedicated Service accounts are used for Web Services, as apposed to SSO or Dimensions user accounts, a Named License is recommended to ensure a lack of an available license does not cause a failure.
	Dimensions RM User Names and Passwords Before upgrading, make sure that you know the passwords for the following accounts: ■ ICDBA ■ ICADMIN If these passwords are not known to you or to a member of the RM team, then re-set them before moving forward with the install.
	Schedule RM Work Stoppage - Stop the RM Pool Manager Service Each RM instance must be backed-up before the installation is begun. In order to ensure that no changes are applied to RM instances once the backup has started we strongly recommend that the administrator schedule RM downtime and then revoke user access by stopping the RM Pool Manager Service.
	Ensure you have Micro Focus Auto Pass Licenses RM versions prior to release 12.10 used the Serena License Manager (SLM). As SLM is no longer supported, ensure that you have Micro Focus Auto Pass installed and that licenses are available. To convert your Serena License Server licenses into Auto Pass licenses, contact Micro Focus support. For further information see: "Licensing" on page 123.

Checklist Items Before Upgrading Dimensions RM Server

✓

	Consider Denial of Service (DOS) Protection As with any solution accessible via the Internet, you might consider protections from denial of service attacks. Some services function as a reverse proxy, which would protect the Dimensions RM server from a Denial of Service attack.
	Upgrade Microsoft Office to a supported version **IMPORTANT!** Ensure that the version of the Microsoft Office is supported by Dimensions RM. To check supported versions, see the Dimensions RM Platform Matrix, https://www.microfocus.com/documentation/dimensions-rm/.
	Upgrade your RDBMS to a supported version **IMPORTANT!** Ensure that the version of the RDBMS is supported by Dimensions RM. To check which version is supported, see the Dimensions RM Platform Matrix. For the installation process of the supported version, see the relevant database chapter as well as "Create and Restore Instances in New Database" on page 100.
	Oracle only: 64-bit Oracle Administrator Client on Application Server For installation of the 64-bit Oracle Client, see chapter "64-Bit Oracle Client Installation in an Upgrade Scenario" on page 132.
	Oracle only: 64-bit Oracle Administrator Client on Web Server The Web server uses a 64-bit Oracle Call Interface (OCI) to communicate with Dimensions RM; therefore, a 64-bit Oracle Administrator client must be installed on the same machine as the Web server. You can verify if the client components are present by connecting through sqlplus. For installation of the 64-bit Oracle Client, see chapter "64-Bit Oracle Client Installation with a Fresh Installation" on page 133.
	MS SQL Server only: 64-bit ODBC System DSN on Application Server A 64-bit ODBC System DSN based on SQL Server Native Client 11 driver must be installed on the Dimensions RM application server. For configuration, see chapter "Configuring the System DSN" on page 145.

Pre-Upgrade Tasks

Record the Dimensions RM Mail Configuration

1 Log in to the Dimensions RM server machine as a system administrator.

2 Record the RM Mail configuration:

a Select:
`(Windows) Start | Open Text | Dimensions RM <version> | RM Mail`

```
Configuration
```

b Click through the **RM Mail** dialog tabs, and take screen shots or write down all of the configuration information, for example:

- Database location.
- Instances.
- Server port number.

NOTE Restoring of e-mail rules to a new database is not supported.

Back up Database, Instances, and Necessary Files

CAUTION!

Before beginning the upgrade, make sure that you have a reliable backup of the RDBMS database installation. In order to create a reliable backup you must ensure that no users are accessing Dimensions RM during the execution of the backup. To ensure this, stop the following services:

- Open Text Common Tomcat
- Open Text Dimensions RM Pool Manager
- Open Text Dimensions RM E-Mail Notification Service

Note that stopping Open Text Common Tomcat will disable all applications using this service.

A Note if also Upgrading the Database Version

If the team is migrating to a new database release in conjunction with the Dimensions RM upgrade. Make a note of the Instances that should be reloaded with the migration, and restore these instances using RM Manage.

Yes, you should backup the database itself, but to reset all connections between Dimensions RM and the data the **restore** must be done using **RM Manage.**

At **import time**, you may be prompted to enter the *From User* with each instance restore, the "From User" refers to the instance name.

For Oracle:

Assuming that the organization's process was to allow RM to create and manage the tablespace when creating new instances – the tablespace name will also be the instance name.

However, if there is an internal process defined for creating an Oracle tablespace for each new RM instances – the tablespace name may differ from the instance (user) name.

- If unsure, from RM Manage, right click on the database name, and select **Administer Tablespaces**. to list the instance name as well as the size of each instance tablespace.

- If, after migration, the instance will remain active, double the tablespace to be assigned when the new instance is created.

Backup all RM instances.

NOTE If installing the new release of RM on the same server, without a change in the RDBMS, the backups will only be re-imported in the event of a problem.

For **MS SQL** the backup is performed at the database level. Using **RM Manage** right click on the database, enter the system administrator password and perform the backup as described below.

For **Oracle** and **PostgreSQL** the backup is performed at the individual instance level. Using RM Manage, right click on the each instance, and select **Backup/Restore Instance Account**, enter the system administrator password when prompted.

RM Manage Backup Dialog	
Field	**Description**
Legacy/Compatibility Mode - **Oracle Only**	Legacy mode formats the backup such that it is compatible with Oracle 10. Legacy must be used when backing up instances from Oracle 10, and must then be used for their import - no matter which release of Oracle the instances are migrated to.
	CAUTION! If Oracle 10 is not in use: **Do not check the legacy box.**
Oracle Backup Path	For Oracle, this field is automatically populated with the default backup path on the Oracle server.
Backup Path	For other supported database, the path should default to the standard path used for "Saved Instances".
File Name	This field is automatically populated with a name for the backup file. The name is based upon the instance name and the current date and time. Edit this name as needed. **TIPS** ■ Note the location to which you saved the files. You may need to browse to that location from the Import dialog of the new RM installation or copy the files to the location expected by the new RM installation. ■ You might want to consider modifying the backup file name such that the reason for this backup is clear, for example: RMDEMO_20230118_FinalFor1211Upgrade.dmp
Security Data	Checking this box will exports all the users that have been assigned to this instance, as well as their permissions, ensuring that this information is imported into another database or instance.
Legacy Mode / Buffer Size	**NOTE** This sets the temporary space available for the operation, and is used for Legacy Mode only. There is no reason to change the buffer size for the backup.

c Click the **Backup** button. If you have not already done so, rename the backufile such that it can be easily differentiated from standard instance backups.

NOTE The log file is saved in the directory where the backup was created. It has the same name as the instance, but with a .log extension instead of a .dmp extension. It also includes the letters "Exp" and a time stamp based on the backup operation, e.g. *InstanceName_ExpDate_ExpTime*_Exp.log

d For **Oracle and PostgreSQL** repeat the preceding steps for each instance. For **MS SQL** the backup is performed at the database level.

Backup all RM Files

a Because some modified configuration files may be overwritten during the install, please **copy the** current **RM directory tree to a backup**. ***For example*** (all in one line):

```
copy "C:\Program Files\Micro Focus\Dimensions 12.11\RM"
C:\RM12.11_Backup
```

b **Also copy the tomcat directory tree to a backup**. For example (all in one line):

```
copy
"C:\Program Files\Micro Focus\Dimensions 12.11\Common Tools 2.3.0
.0\tomcat" C:\RM12.11_tomcatBackup
```

Ensure that all RM related Services have been stopped:

Please be aware that this release includes re-branding of Dimensions RM. What was once, Micro Focus Common Tomcat, for example, is now Open Text Common Tomcat.

We will be stopping the following - but starting them, when the installation is complete, under the new Open Text brand.

- Micro Focus ALF Event Emitter
- Micro Focus Common Tomcat
- Micro Focus Dimensions RM E-Mail Notification
- Micro Focus Dimensions RM Pool Manager
- Micro Focus SyncEngine

Stop RM related Processes

- rmLicenseAgent.exe

Uninstall Dimensions RM

1 Uninstall the existing Dimensions RM version using **Add or Remove Programs** from the Windows Control Panel.

2 Following the Dimensions RM uninstall, please check that the **Micro Focus Common Tomcat** associated with Dimensions RM has also been uninstalled. If this is not the

case, uninstall **Micro Focus Common Tomcat** using **Add or Remove Programs** from the Windows Control Panel.

Check RDBMS Clients

Oracle only: 64-bit Oracle Administrator Client on Web Server

As of Dimensions RM version 12.8, RM server and RM Admin tools are 64-bit applications and require 64-bit access to the Oracle database. Any version prior to RM 12.8 required a 32-bit Oracle client, the 32-bit client must be uninstalled before proceeding with the installation.

For installation of the 64-bit Oracle Client, see chapter "64-Bit Oracle Client Installation in an Upgrade Scenario" on page 132.

MS SQL Server only: 64-bit ODBC System DSN on Application Server

A 64-bit ODBC System DSN based on SQL Server Native Client 11 driver must be installed on the Dimensions RM application server. For configuration, see chapter "Configuring the System DSN" on page 145.

Upgrade Microsoft Office to a supported version

Ensure that the installed version of the Microsoft Office is supported by Dimensions RM. To check which version is supported, see the Dimensions RM Platform Matrix.

Install Dimensions RM

Please follow the instructions in Chapter 5, "Server Installation - Final Checks" on page 52. Once the installation is complete, return to complete the **Post-Upgrade Tasks.**

Post-Upgrade Tasks

Check Installation has completed successfully

There is a small possibility that the installation may not have completed successfully even though it may have appeared to have done so. It is recommended that you check that the expected software is listed in the `Control Panel | Add or Remove Programs` window following the installation. The appropriate version should be: **Dimensions RM 12.11.2 (23.4)**.

Check Windows Services

1 Log in as a user with local Windows administrative rights. Access and display services by:

`Start | Control Panel | Services`

or

`Start | Control Panel | Administrative Tools | Services`

2 Check that the following database and Dimensions RM services have Status `Started` and that Startup is `Automatic`.

- Dimensions RM services:

  ```
  Micro Focus Dimensions RM Pool Manager
  Micro Focus Common Tomcat
  ```

  `Auto Pass License Server`: This service may be absent if you are using Micro Focus Auto Pass on another server. If the service is present and is not running, start it.

- **Database Related Services:** Whether Oracle, SQL Server (MSSQLSERVER) or PostgreSQL Server - check to be sure that related services are active

3 Open Windows Task Manager and check for the following Dimensions RM processes:

- Dimensions RM processes:

  rmAppServer.exe
  `RMServerPool.exe`

Restore Files from Backup

Security.dat

Copy the `security.dat` file from the `RM` directory of your backup to the `RM` directory of your server installation.

sts.pem

The `sts.pem` file only exists if you configured Single Sign-On (SSO), and have included SSO in your upgrade. If you are not using SSO, skip this step.

Copy the `sts.pem` file from the `RM\conf` directory of your backup to the `RM\conf` directory of your server installation.

Copy Configurations

Copy the **conf** folder (from the backup of the **rtmBrowser** directory) to your new rtmBrowser setup.

Copy

```
C:\MyBackup\Dimensions RM\Common Tools
#.#.#.#\tomcat\#.#\webapps\rtmBrowser\conf
```

to

```
C:\Program Files\Open Text\Dimensions 12.11.2\Common Tools
2.3.0.0\tomcat\9.0\webapps\rtmBrowser\conf
```

Copy Forms

When using custom forms, copy the folders inside the **forms** folder (except the **common** folder) to your new rtmBrowser setup. The folders to copy have the same name as your database instance. If your database instance is named ORCL, you would have to copy the ORCL folder (if it exists). The example below will use ORCL as database name.

Copy

```
C:\MyBackup\Dimensions RM\Common Tools
#.#.#.#\tomcat\#.#\webapps\rtmBrowser\forms\ORCL
```

to

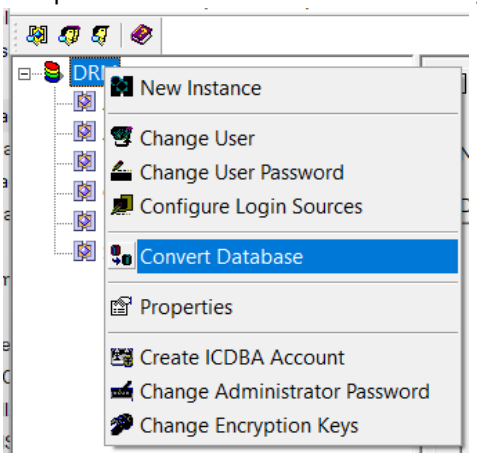
```
C:\Program Files\Open Text\Dimensions 12.11.2\Common Tools
2.3.0.0\tomcat\9.0\webapps\rtmBrowser\forms
```

Convert (Upgrade) Database and Instances

The database and the RM instances must be converted when upgrading Dimensions RM, as well as when restoring an instance created with an older version of Dimensions RM.

To convert the database or an instance, do the following:

1. Right-click on RM Manage, and select **Run as administrator** from the context menu.
2. Right click on the Dimensions RM database in the left-hand graphical tree and select Convert Database. This opens the Database Validation Dialog.



3. To expand the database that contains the instance you want to convert, click +.
4. Enter the ICDBA pass word when prompted.
5. Confirm the automatic update request by clicking yes, or update the database manually by selecting the database and then clicking **Upgrade**.
6. To upgrade each instance:
   - **a** Select the first instance, all will need upgrading.
   - **b** Click **Upgrade**. This opens the **Conversion Progress** dialog.
   - **c** Click **Continue** to start the conversion process, and continue through each instance until all have marked: Current.
   - **d** **Close** to close the **Database Validation** dialog.

Test Browser Access

1. Open a web browser.
2. Enter the URL to your Dimensions RM server into the URL box. The following URLs should work on the server:

- `http://localhost:8080/rtmBrowser/`
- `https://localhost:8443/rtmBrowser/`

If you modified the ports during installation, use the ports specified.

If there are any issues, please contact Micro Focus Support. Please include details and, if possible, screen shots describing the issue.

Configuring HTTPS

If SSO and/or HTTPS were configured prior to this upgrade, and the proper SSO selection was made during setup, returning that configuration (from your backup files) should restore the implementation as it once was.

However, if making changes to your configuration or addressing issues please refer to the chapter "Configuring Tomcat", Section *"Working with Secure Socket Layers"* in the *Administrator's Guide*.

You may also contact support: http://supportline.microfocus.com. Please include details and, if possible, screen shots describing the issue.

Ensure Dimensions RM is excluded from Anti-Virus

It is recommended that certain files be excluded from real-time checking for all reads and writes. Please see "Virus Checkers" on page 64 for a list of files to be excluded.

Check Configuration for Export/Import

Dimensions RM provides export functions to Word, Excel, and PowerPoint to ensure proper configuration please see

Install the Latest Patch

If you have not already done so, please check for any patches available with the Dimensions RM installation, see "Checking for Latest Updates" on page 43.

It is best to complete the application of patches before turning the release over to the user community.

New Groups: System and Instance Administrator

Please note that as of release 12.11 there are two types of Administrator defined in Dimensions RM: **Administrator** and **System Administrator. The role you play depends upon the group you are in.**

The **Administrator** (Instance Administrator) is responsible for administrator functions within the boundary of the **assigned instance**.

For example, from the RM Browser, the Administrator may:

- Create users and groups, but have no visibility of users ot groups beyond their own instance

- Modify the instance schema and attribute settings,
- Define and/or modify categories
- Set default instance settings

The **System Administrator** is able to perform all Administrator functions as well as to administer all configuration settings valid for the RM installation, for example:

- All Instance creation, modification, and deletion,
- User and Group management across all Instances,
- Access to RM Browser administrative tools.

Chapter 3

Installing Dimensions RM Server

Pre-Installation Checklist

Micro Focus **strongly recommends** to use the following checklist when preparing to install the Dimensions RM server as to avoid skipping important steps.

✓ Checklist Items Prior to Installing Dimensions RM Server

	Download the Platform Matrix Download the Platform Matrix at https://www.microfocus.com/documentation/dimensions-rm/ Use the platform matrix to ensure support for the following: ▪ **Supported Windows Operating System** ▪ **Supported Microsoft Office Version** ▪ **Supported Web Browser** ▪ **Supported databases**; if upgrading the database as well as Dimensions RM, please see associated instructions ▪ For **Dimensions CM Integration**: Supported Dimensions CM Client versions
	Downloading the 12.11.2 (23.4) release of Dimensions RM and Latest Patch When downloading the installation zip file, please include the release notes, the ReadMe file, and the associated documentation from the Micro Focus support website. From the release notes and the ReadMe files you will find the most up-to-date list of enhancements and defects corrected in the release. You can't benefit from features you don't know about! Micro Focus support website: http://supportline.microfocus.com For downloading the latest patch, see "Checking for Latest Updates" on page 43.
	RAM / CPU / Disk-Space Recommendations For recommendations on RAM, CPU power, or Disk space, see the Dimensions RM Readme file.
	Consider Denial of Service (DOS) Protection Especially when having Dimensions RM accessible from Internet — but also for internal servers — it should be considered to protect the Dimensions RM server from DOS attacks. For this, you might consider implementing a cloud-based protection. You could use a service that can function as a reverse proxy, which — as a result — would protect the Dimensions RM server.

✓ Checklist Items Prior to Installing Dimensions RM Server

	Licensing Dimensions RM: First Time Install If installing a fully licensed release of Dimensions RM, you must install Micro Focus Auto Pass release 11.5 or higher before installing Dimensions RM. RM release 12.11.2 (23.4) will not function with an older Auto Pass version. Ensure that AutoPass port (default is 5814) is open for inbound connections on the AutoPass server Ensure that AutoPass port is open for outbound connections on the RM server For additional details about licensing Dimensions RM, see: "Licensing" on page 123. For AutoPass documentation see https://docs.microfocus.com/itom/AutoPass_License_Server:latest/Home. For evaluations there is a 30-day license option that may be selected during RM installation.
	Named Web Service License If Dedicated Service accounts are used for Web Services, as opposed to using user accounts, assigning a Named User License is recommended to ensure a lack of an available application license does not cause a failure.
	For Oracle: Install a Supported Database ■ For Oracle: see "Installing and Configuring Oracle" on page 127. ■ Prior to RM Installation, a database instance on the Oracle server must be created. ■ **Ensure that the 64-bit Oracle Client has been installed on the Application Server.** See chapter "64-Bit Oracle Client Installation with a Fresh Installation" on page 133. ■ **Install the 64-bit Oracle Client has been installed on the Web Server.** The Web server uses a 64-bit Oracle Call Interface (OCI) to communicate with Dimensions RM; therefore, a 64-bit Oracle Administrator client must be installed on the same machine as the Web server. You can verify if the client components are present by connecting through sqlplus.
	For MS SQL Server: ■ For MS SQL see "Installing and Configuring MS SQL" on page 139. ■ **A database instance on MS SQL server must be created prior to the installation of Dimensions RM.** ■ **A 64-bit ODBC System DSN based on SQL Server Native Client 11 driver** must be installed on the Dimensions RM application server as described in chapter "Configuring the System DSN" on page 145.

✓ Checklist Items Prior to Installing Dimensions RM Server

	PostgreSQL: **PostgreSQL can be installed and configured on the same machine as Dimensions RM in conjunction with the installation of Dimensions RM.** Alternatively, a local installation may be configured. ■ For PostgreSQL see "Installing and Configuring PostgreSQL" on page 147. ■ **A database instance on PostgreSQL server must be created prior to the installation of Dimensions RM.** ■ **If the PostgreSQL database is installed on a different machine**: • It must be configured to allow access from the Dimensions RM server. For details, see chapter "Accessing PostgreSQL from other Machines" on page 151. • The PostgreSQL command line tools must be installed. For details, see chapter "Installing the PostgreSQL Command Line Tools" on page 149.
	IPv6 Support When operating in an IPv6-only environment, IPv4 must be installed on the server running Dimensions RM. It is not required to enable IPv4 after installing it.
	Note Server Host Names Unless installing all components on the same server, please make note of the names of the machines hosting the database and Micro Focus Auto Pass. This information must be supplied during installation.
	Microsoft Office Microsoft Office must be installed on the Dimensions RM server to support browser-based Word import, document export, RM Import, and RM Import Designer tools. For further information, see chapter "Microsoft Office Requirements" on page 17.
	LDAP Server Although this information can easily be added later, if the organization is intending to use the LDAP login source, identify the LDAP server and port.
	Planning your Dimensions RM user names and Passwords Before this first-time installation, please plan for your Dimensions RM user names and define a strategy for managing their passwords. The first critical user names are the ICDBA and ICADMIN accounts; these are not login accounts, but their passwords are required for certain system administrator tasks. There are also passwords required for each database instance created, it is particularly useful to define a strategy for assigning passwords to these objects.

✓ Checklist Items Prior to Installing Dimensions RM Server

	Defining Users for System and Instance Administration Please note that as of release 12.11 there are two types of Administrators defined in Dimensions RM: **Administrator** and **System Administrator. The role you play depends on the group you are in.** The **Administrator** (aka Instance Administrator) is responsible for administrator functions within the boundary of the assigned instance. For example, from the RM Browser, the Administrator may: • Create users and groups, but have no visibility of users ot groups beyond their own instance • Modify the instance schema and attribute settings, • Define and/or modify categories • Set default instance settings The **System Administrator** is able to perform all Administrator functions as well as to administer all configuration settings valid for the RM installation, for example: • All Instance creation, modification, and deletion, • User and Group management across all Instances, • Access to RM Browser administrative tools.
	E-mail Notification If installing the e-mail notification service, you must know the name of the computer running the service and the name of the SMTP mail server to be used. This feature may be implemented at any time following the full installation.

Installing Dimensions RM

Please follow the instructions beginning with: Chapter 5, "Server Installation - Final Checks" on page 52. Once the installation is complete, return here to complete the **Post-Installation Tasks.**

Post-Installation Tasks

Check Installation has completed successfully

There is a small possibility that the installation may not have completed successfully even though it may have appeared to have done so. It is recommended that you check that the expected software is listed in the `Control Panel | Add or Remove Programs` window following the installation. The appropriate version should be: **Dimensions RM 12.11.2 (23.4)**.

Check Windows Services

1 Log in as a user with local Windows administrative rights. Access and display services by:

```
Start | Control Panel | Services
```

or

```
Start | Control Panel | Administrative Tools | Services
```

2 Check that the following database and Dimensions RM services have Status `Started` and that Startup is `Automatic`.

- Dimensions RM services:

  ```
  Micro Focus Dimensions RM Pool Manager
  Micro Focus Common Tomcat
  ```

  `Auto Pass License Server`: This service may be absent if you are using Micro Focus Auto Pass on another server. If the service is present and is not running, start it.

- **Database Related Services:** Whether Oracle, SQL Server (MSSQLSERVER) or PostgreSQL Server - check to be sure that related services are active

3 Open Windows Task Manager and check for the following Dimensions RM processes:

- Dimensions RM processes:

  rmAppServer.exe
  `RMServerPool.exe`

Configuring SSO and/or HTTPS

If the Open Text SSO was selected during this installation, please follow the instructions in Section in "SSO and CAC Configuration" on page 70.

If Open Text HTTPS was selected during this installation, please see Section "Configuring SSL Certificates" on page 72

If there are questions or issues, please contact support: `http://supportline.microfocus.com`. Include details and, if possible, screen shots describing the specific location of the issue encountered.

Configuration and the First Instance

The newly created RM database requires additional configuration before it can be accessed. This configuration is performed using the newly installed administration tool: RM Manage.

During configuration the administrator account ICDBA is created. This account is not a log in account, but access to it is required for administrative tasks such as new instance creation. The creation of the ICDBA account requires a database administrator account.

- **Oracle:** An account which belongs to the sysdba group.
- **MS SQL Server:** An administrator account, such as the built-in sa account or a Windows administrator account for the domain or server.

- **PostgreSQL**: An administrator account, such as Postgres, or a similarly privileged account without superuser privilege.

RM Manage *can be* accessed from a desktop icon, or from:

```
Start | All programs | Open Text | Dimensions RM 12.11.2  (23.4) | RM Manage
```

RM Manage

1 Right-click on RM Manage, and select **Run as administrator** from the context menu.

2 Create the ICDBA account:

a Right-click on the database instance configured for RM, RMQP02 in the examples, and select **Create ICDBA Account**.

b Enter the ICDBA password. The existing SYSDBA account and password must be entered for authentication.

c Click on **Advanced**: For this initial RM Demo instance 2048 MB is sufficient. When creating production databases, increase the tablespace size to 2 GB for general usage and 4-6 GB for installations with more than 20 users.

d Click on **Create**

If the DBA has chosen to create a tablespace for each RM instance in advance of instance definition (Create in an existing tablespace) use the sizes mentioned above.

3 From RM Manage, create a "New Instance" – as the first instance in the database the process for its creation is unique. The RMDEMO sample instance should be used to "prime" the database. It provides an excellent example of a "typical" instance definition - however it should not be used to initiate an instance.

a Right-click on the database and select **New Instance**.

b The user is prompted to enter the ICDBA account password.

c The user will be prompted to set the ICADMIN password. The ICADMIN account is NOT a login account.

d The next step is to name the instance, RMDEMO, and to set the RMDEMO instance administrator account password. This administrator account allows for a separation of administrator duties between accounts. Using RMDEMO, Enter instance name and establish instance admin password; click **OK**.

NOTE Make a note of the instance administrator password – you will need this soon.

e From the **Sample Instances** tab, select **RMDEMO**.

f Unless you would like to allow users to "play with this instance" using fake user names, do not check **Include Security Data**.

g Set **Buffer Size** to 100.

h Click **Install**.

i If the message *The version of instance "RMDEMO" is not current. Would you like to update it now?* is displayed – click **Yes**.

4 Once the RMDEMO instance has been created and populated, a minor version inconsistency.will be displayed. Please convert the database before continuing.

a To convert, right-click on the database name and select **Convert Database**.

b Highlight the database, for example RMQP02, and select upgrade.

c Click **Yes** when prompted to re-create procedures.

5 After the conversion has completed, the instances within it must be upgraded.

a Click on the **+ sign** to expand the instance list – for an initial installation. There will only be RMDEMO.

b Highlight the RMDEMO instance and click on **Upgrade**.

c When the *Conversion Progress* dialog is raised, click on **Continue**.

d Click on **Done**, when the selection is no longer grayed out.

6 For a new installation, the user will be prompted to *Change User*; change the user to the admin account created with the RMDEMO instance. The user name is *RMDEMOAdmin* and the password is that which was set when the instance was created.

Ensure Dimensions RM is excluded from Anti-Virus

It is recommended that certain files be excluded from real-time checking for all reads and writes. Please see "Virus Checkers" on page 64 for a list of files to be excluded.

Check Configuration for Export/Import

Dimensions RM provides export functions to Word, Excel, and PowerPoint to ensure proper configuration please see "Support for Export/Import" on page 76.

Additional Oracle Database Checks

Permissions of the ICDBA Account

The ICDBA account must have the Create Any Context and the Execute on sys.dbms_session rights. By default, ICDBA is created as a database administrator and therefore has these rights. If you create ICDBA manually, you may have to grant these rights with the following commands:

- `GRANT CREATE ANY CONTEXT TO ICDBA`
- `GRANT EXECUTE ON sys.dbms_session TO ICDBA`

Password Expiration for Oracle Passwords

The standard security default for passwords on Oracle is to expire after 180 days. If your passwords expire you will receive an ORA-28001 error message. Your DBA should ensure that Oracle accounts are created so that they do not expire. You should also update the `security.dat` file in `<install directory>\Open Text\Dimensions <version>\RM\` on a regular basis.

The passwords for the Dimensions RM database administrator Oracle accounts `ICDBA` and `ICADMIN` can be changed from within RM Manage — see "Changing Database Administrator Account Passwords Using RM Manage" on page 42.

For other Oracle accounts, the following SQL script can be run when creating them such as to disable password expiration, but this will only work if run prior to a password actually expiring.

CAUTION! Micro Focus makes no warranty of any kind in regard to the contents of this script, including but not limited to implied warranties of merchantable quality or fitness for any particular purpose. Micro Focus shall not be liable for errors contained in it or for incidental or consequential damages in connection with the furnishing, performance, or use of this script. The information in this script is subject to change without notice.

Script start

```
/*
With Oracle, the security defaults set Oracle Account to expire the
    passwords after 180 days. This forces the user to change all DB
    passwords for Oracle accounts
   sys
   system
   ICDBA
   ICADMIN
   <RM Instances>
This is good default security but requires good Oracle knowledge to
    maintain these accounts. As a work around this script creates a
    profile where passwords will NOT expire. Then assigns account RM
    needs to this profile. This must be run before the account have
    their password expire. Once the passwords expire they must be
    changed.

Please be aware that by running this script you are reducing the
    security of the Oracle database. Be sure you understand the risks
    and accept them before running this script.
*/

CREATE PROFILE "MICROFOCUSNOLOCKOUT" LIMIT CPU_PER_SESSION DEFAULT
   CPU_PER_CALL DEFAULT
   CONNECT_TIME DEFAULT
   IDLE_TIME DEFAULT
   SESSIONS_PER_USER DEFAULT
   LOGICAL_READS_PER_SESSION DEFAULT
   LOGICAL_READS_PER_CALL DEFAULT
   PRIVATE_SGA DEFAULT
   COMPOSITE_LIMIT DEFAULT
   PASSWORD_LIFE_TIME UNLIMITED
   PASSWORD_GRACE_TIME UNLIMITED
   PASSWORD_REUSE_MAX 1
   PASSWORD_REUSE_TIME UNLIMITED
   PASSWORD_LOCK_TIME 5
   FAILED_LOGIN_ATTEMPTS UNLIMITED
   PASSWORD_VERIFY_FUNCTION NULL
;
```

```
/*
As a minimum the ICADMIN account should be set to not expire as these
    accounts do not receive pending expiration warnings. They are more
    involved to change than the others requiring generation of a new
    Security.DAT file.
*/
ALTER USER ICADMIN PROFILE MICROFOCUSNOLOCKOUT;
/*
Next set the primary RM accounts: ICDBA and the INSTANCES to not expire.

Below please copy and edit the line
     ALTER USER RMDEMO PROFILE MICROFOCUSNOLOCKOUT;
Change RMDEMO to your first instance name - uppercase
Then copy this line so each instance has its own line.
*/
ALTER USER ICDBA PROFILE MICROFOCUSNOLOCKOUT;
ALTER USER RMDEMO PROFILE MICROFOCUSNOLOCKOUT;

/*
And lastly the Main Oracle accounts. This is where the security starts
    to get weak if you do not change the passwords on a regular basis.
    If you do not have a DBA to maintain these for you it may be good to
    make sure they do not expire and lockout.Especially as the RM admin
    you will rarely use these accounts.
*/
ALTER USER SYS PROFILE MICROFOCUSNOLOCKOUT;
ALTER USER SYSTEM PROFILE MICROFOCUSNOLOCKOUT;
ALTER USER SYSMAN PROFILE MICROFOCUSNOLOCKOUT;
ALTER USER DBSNMP PROFILE MICROFOCUSNOLOCKOUT;

Script end
```

Changing Database Administrator Account Passwords Using RM Manage

The passwords for the Dimensions RM database administrator accounts `ICDBA` and `ICADMIN`, can be changed from within RM Manage.

To change the ICDBA or ICADMIN account password:

1. Select the database whose administrator accounts (one or more of ICDB or ICADMIN) you want to change associated passwords.
2. Select **File** | **Change Administrator Password**, click the **Change Administrator Password** button  , or right-click the database and select **Change Administrator Password**.
3. The **Change administrator password** dialog box opens.
4. In the **Select account to modify area**, select the `ICDBA` or `ICADMIN` as appropriate from the **Account** drop-down list.

5 In the **Change account password** area, type the new password that you want to assign to the chosen account.

IMPORTANT! The password must be in upper case only.

6 In the associated **Confirm Password** field, re-type the password.

7 In the **Enter ICDBA account password** area (note for ICDBA, this will be entitled **Enter current ICDBA account password**), type the current ICDBA password.

8 Click **Change**.

IMPORTANT! For the Oracle RDBMS, Oracle account passwords expire by default after 180 days. Unless your DBA has re-configured such RDBMS to override this default and allow permanent passwords, you must change the ICDBA password before 180 days elapse.

Checking for Latest Updates

After installing Dimensions RM, it is suggested that you periodically visit the Micro Focus support Web site at

http://supportline.microfocus.com

This site will list corrections or minor enhancements associated with the release. First time users must register for a user name and password.

Once logged into the support site, under `Licenses & Downloads` you will find an option to download available releases, as well as any existing patches. As a last step in the installation, it is recommend that any existing patches be included. Check the instructions associated with the patches, it is often the case that the latest is all-inclusive.

Continuing with the Setup

Please proceed to the Administration Section of the Dimensions RM Browser to continue with setup, including defining groups and users.

Chapter 4

Installing the Administrator Client

Preparing for Installation

The instructions for Installing the RM Administrator Client, including RM Import Designer and RM Import, apply to both the Installation and Upgrade.

Micro Focus **strongly recommends** to use the following checklist when upgrading the Dimensions RM Admin Client as to avoid skipping important steps.

IMPORTANT! The check list below requires that your current Dimensions RM installation is of version 12.8.1 or higher. If you wish to upgrade any version older than 12.8.1, please contact Micro Focus support.

Pre-Installation Tasks	
	Download the Platform Matrix Download the Platform Matrix at https://www.microfocus.com/documentation/dimensions-rm/
	Supported Windows Operating System To check that the client version of Windows is supported, please see the Platform Matrix.
	Supported Microsoft Office version To check that the client version of Microsoft Office is supported, please see the Platform Matrix. If your version of Microsoft Office is not supported or you do not have Microsoft Office installed, the RM Import tool will not be available.
	Accessing the 12.11.2 (23.4) release of Dimensions RM and Latest Patch **Important! The version and patch level for the RM Admin Client Installed must be consistent with both version and patch installed on the server.** If the installation and patch zips are available on your server, please copy those to the client for installation, otherwise download once again, paying careful attention to the version and patch level. Micro Focus support website: http://supportline.microfocus.com

If this is the initial installation of the Admin Client, please proceed to "Installing the RM Admin Clients" on page 47

Before Upgrading the RM Admin Client

Prior to initiating the installation, please uninstall the currently installed version of the Dimensions RM Client applications. Once completed, please restart the machine.

Depending on the database accessed by the Dimensions RM Server, please perform one of the following:

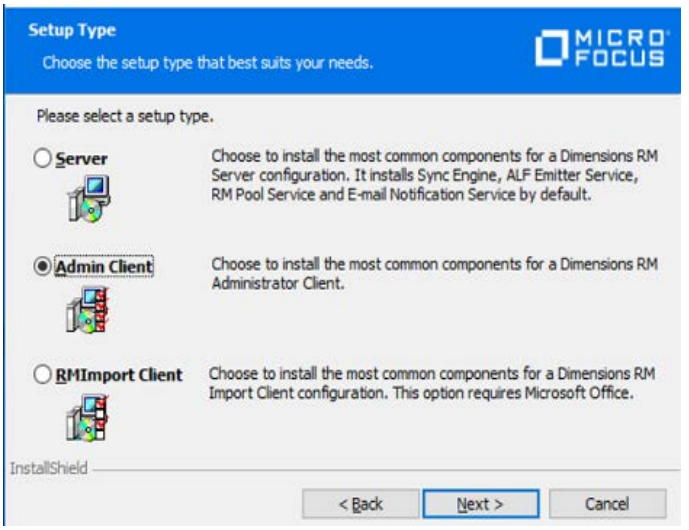
- If Oracle:

- If the previously installed version of Dimensions RM used the 32-bit Oracle Client, please uninstall the 32-bit Oracle Client
- Install the 64-bit Oracle Administrator Client on the Client machine. Instructions can be found in chapter "64-Bit Oracle Client Installation in an Upgrade Scenario" on page 132.

- If MS SQL Server:
  - A 64-bit ODBC System DSN may already be installed, if not please see chapter "Configuring the System DSN" on page 145.
- If PostgreSQL Server:
  - If the PostgreSQL ODBC driver has not yet been installed see chapter "Installing and Configuring the ODBC Driver" on page 153

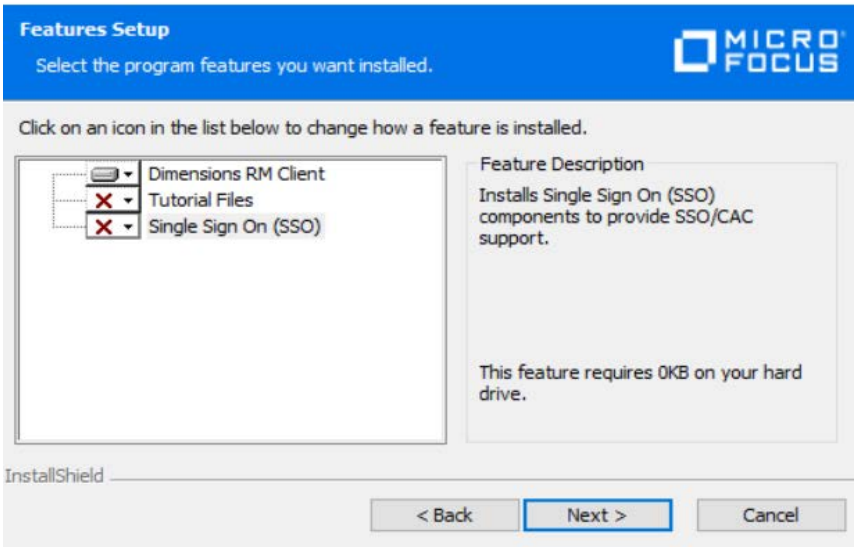
Installing the RM Admin Clients

1. From the same downloaded release package used to install Dimensions RM on the server, right-click on the file: `setup.exe` and choose **Run as administrator** from the context menu. This opens the Dimensions RM installation wizard.
2. Click **Next**.
3. Select **I accept the terms of the End User License Agreement** and click **Next**.
4. Select Admin Client. Please note that the RM Import Client will not install on a system on which Microsoft Office has not been installed.



5. **Destination Folder:** Accept or To Change:
   a. Click **Change...** to open the **Change Current Destination Folder** dialog.
   b. Select the drive and/or directory to install to.
   c. Click **OK**.
6. Click **Next**.

7 In the **Features Setup** dialog choose, by selecting the **red X** items that should **not** be installed. Choosing Dimensions RM Client, as shown below, will install RM Manage, making System Administration available to administrators without the need to log onto the server. The Tutorial Files are a copy of those downloaded with the Server, choosing not to download them with the install.



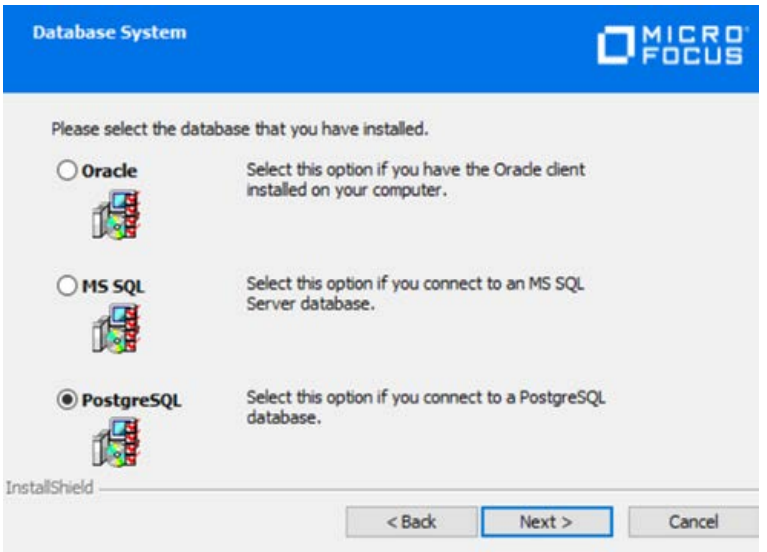
8 Click **Next**.

9 Specifying RM Server and Port

Specify the Host Name or IP address of the system on which the Dimensions RM Server was installed.

10 Click **Next**.

11 Select the Database Installed on the Server and click **Next**.



12 Click **Next**.

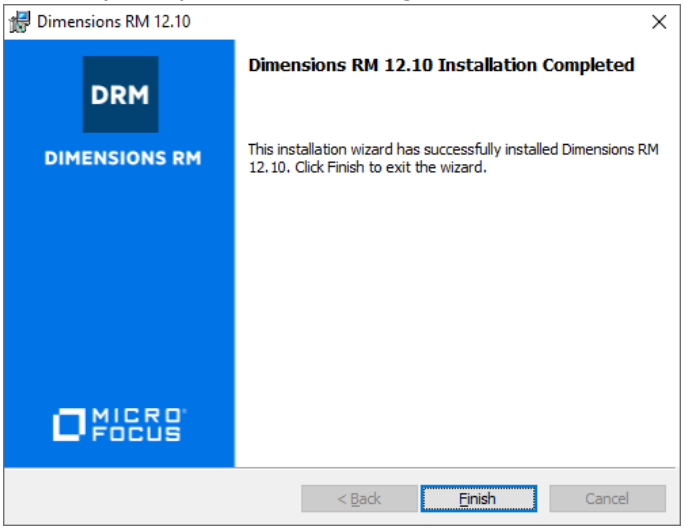
13 Based on database selected, the databases supporting Dimensions RM on the server, submit the database access information

14 Enter the path to the `security.dat` file. This file must be stored under RM in the installation directory tree, for example:
`C:\Program Files\Open Text\Dimensions 12.11.2 (23.4)\RM\security.dat`

15 If you want to see shortcuts for the client applications on the desktop for all users, select the **Add Shortcuts** box.

16 Click **Install** to start the installation process.

17 Once the *Successfully Completed* install dialog is raised, click **Finish**.



18 Copy the secuity.dat file from the RM folder on the server, to the RM folder in the client installation.

19 To test RM Manage, Click on the RM Manage icon  ,if you elected to **Add Shortcuts** or select **Start** | **RM Manage** if you did not.

Assuming the correct identification of the server details and a valid security.dat file, the RM Admin client (RM Manage) should be accessible.

Complete documentation for RM Manage can be found in the *RM Administrator's Guide.*

Testing RM Import Clients

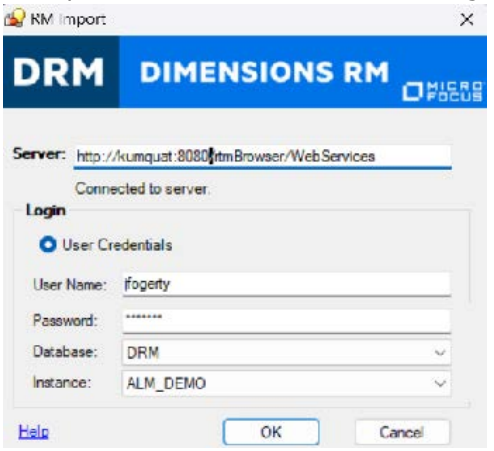
Complete documentation for RM Import Designer and RM Import can be found in the *RM Administrator's Guide*. This section of the Installation Guide has been included in order to test the installation of the Import clients once installed.

If your server installation is using secure socket layers (SSL), a certificate selection dialog may be displayed during the server validation.

Before logging in, you must know the full URL or name and port number of the server running the RM Web service, which, in many cases, will be the the RM Server.

1 Select **Start** | **RM Import** to raise the RM Import dialog.

2 Enter the host name and port number of the server running the RM Web Service,



followed by a tab, which should complete the URL. The full URL may be entered manually, for example: http://kumquat:8080/rtmBrowser/WebServices

3 Click into the User Name box and enter a valid user name; a user with access to at least one Dimensions RM instance.

4 Enter password, select Database, and instance.

5 Click on OK. The initial dialog should be raised allowing the user to choose the import type.

If there are any issues, please contact Micro Focus Support. Please include details and, if possible, screen shots describing the issue.

Chapter 5

Installing Dimensions RM

Installation Types

Installation Types

The following table describes the three installation options available with the Dimensions RM installer; the server installation installs the admin client and import tools. The installation described in this section is focused primarily on the Server Installation.

Option	Description
Server Installation	This installation type will install the Admin Client, Sync Engine, ALF Emitter Service, RM Pool Service and E-mail Notification Service by default, and will make the RM Browser available to the organization. This option requires Microsoft Office (32-bit or 64-bit).
Admin Client	Choose to install the Admin Client, RM Manage, only. This installation type is selected when making the client available on the administrator's desktop.
RM Import Client	Installs the RM Import client, which is used to import files from Microsoft Office. The Dimensions RM components installed are: This option requires Microsoft Office (32-bit or 64-bit), otherwise RM Import will not be available for installation.

Server Installation - Final Checks

Final Assumptions

IMPORTANT! Before continuing with the section, please be sure that you have read and completed tasks described in chapter "Before Installing" on page 9. This includes a review of the checklist, as well as considerations for SSO and Oracle.

The Following are Assumptions: no action needed:

1. Stable OS and Oracle Server
2. Micro Focus Auto Pass must be installed with RM Licenses, unless planning to use the 30-day evaluation.
3. 32-bit or 64-bit edition of Microsoft Office (Word, Excel, PowerPoint, Office tools) has been installed – on the server
4. System Administrator access

   The installation must be **Run As Administrator**

   - If the individual performing the installation does not have privileges – find someone who does.

- The installation updates the registry, full administrator privileges are absolutely necessary for a successful installation.

5 The following examples assume that the product will be installed in:

```
C:\Program Files\Open Text\Dimensions 12.11.2  (23.4)\RM
```

Browse to a different installation folder if desired and note the path difference as you follow the instructions.

Final Tomcat Reminder

IMPORTANT! All Dimensions RM releases install with Tomcat – please check the following before proceeding.

1 Ensure that the RM Tomcat port selected does not conflict with any existing Tomcat installations.

2 The default port is 8080, but an alternate can be specified during installation.

If Dimensions RM is installed on the same server as SBM or Dimensions CM, you must ensure that the Tomcat installed with RM does not conflict with the ports used by SBM and Dimensions CM.

Disabling Admin Approval Mode

1 Open a command prompt.

2 Type `secpol.msc` and hit **Enter**. This opens the local **Security Policy Management Console**.

3 Open the **Local Policies** folder.

4 Select the **Security Options** folder.

5 Double-click **User Account Control: Admin Approval Mode for the Built-in Administrator account**.

6 Set the value to **Disabled**.

7 Click **OK**.

8 Double-click **User Account Control: Run all administrators in Admin Approval Mode**.

9 Set the value to **Disabled**.

Installing the .NET Framework

1 Open **Server Manager**.

2 Click **Next** until **Features** is selected.

3 In the **Features** list, expand one of the following:

- **.NET Framework 4.5 Features**

- **.NET Framework 4.6 Features**

4 Select one of the following:

- **.NET Framework 4.5**
- **.NET Framework 4.6**

5 Click **Next**.

6 Click **Install**.

NOTE RM Import requires Microsoft Office 2010 SP1 or higher to be installed. If you are installing Microsoft Office, also see chapter "Click OK." on page 73.

7 Restart the server.

Installation folders

All examples in this document assume that Dimensions RM is being installed in:

```
C:\Program Files\Open Text\Dimensions 12.11.2  (23.4)\RM
```

Early in the installation process an option is provided to change the default location.

Run Setup.exe as Administrator

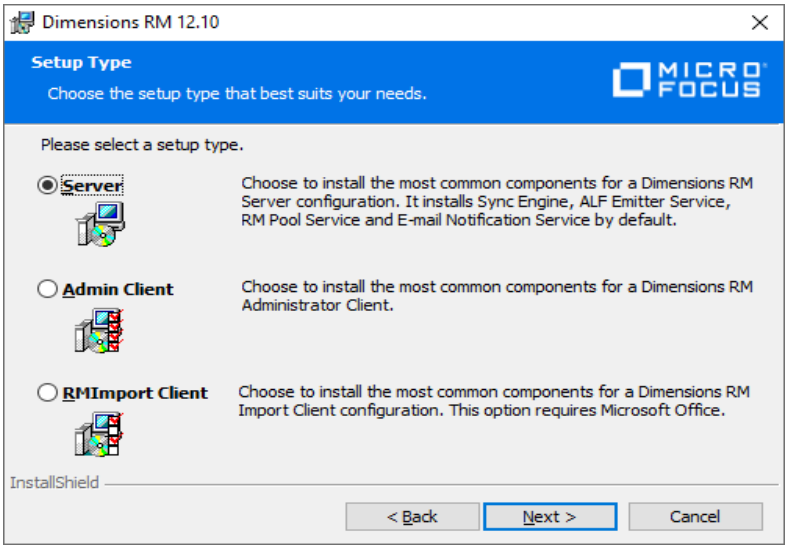
IMPORTANT! If you are running the setup in an environment without Internet connection, you might receive an error message about an invalid file signature. For details, see chapter "Running Setup.exe without Internet Connection" on page 61.

1 From the downloaded release package, right-click on the file: `setup.exe` and choose **Run as administrator** from the context menu. This opens the Dimensions RM installation wizard.

2 Click **Next**.

3 Select **I accept the terms of the End User License Agreement** and click **Next**.

4 Select **Server** and click **Next**.



5 If desired, change the destination folder:

   a Click **Change...** to open the **Change Current Destination Folder** dialog.

   b Select the drive and/or directory to install to.

   c Click **OK**.

6 Click **Next**.

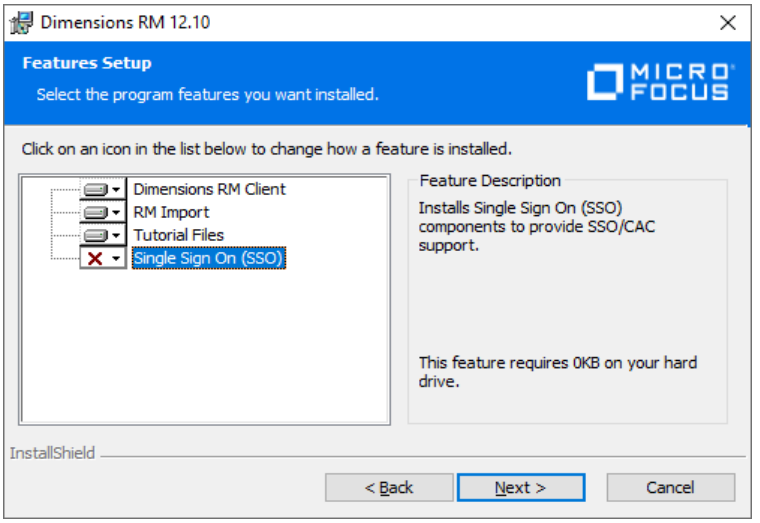
CAUTION!

- When installing Dimensions RM with Open Text SSO, **specify a host name** rather than an IP address. Otherwise SSO may not work correctly with Web applications. The host name **must be exactly the same** configured for the gatekeeper in SBM or Dimensions CM.
- The Dimensions RM SSO installation changes many configuration files to ensure that SSO performs correctly. It is difficult to perform these configuration changes manually. We recommend that if non-SSO configuration is to be modified to support SSO, you might consider re-installing the product, or check with Serena RM Support for assistance.

7 In the **Features Setup** dialog, choose the items that **should not be installed**. When running a server install – the only option is whether or not to include Single Sign On. Keep **Single Sign On (SSO)** selected if you want to use SSO with Dimensions RM.

   - …an SSO enabled Solution Business Manager (SBM) server installation.
   - …an SSO enabled Dimensions CM server installation.
   - …Windows user accounts for web browser login.

   If you do not want to use SSO, de-select **Single Sign On (SSO)**.

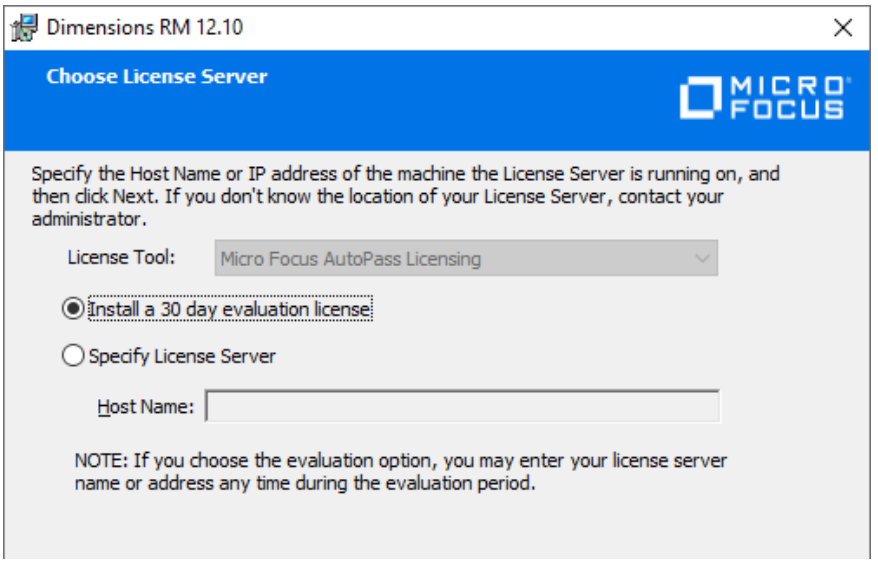


8 Click **Next**.

9 Specifying the License Server

If you have a license server installed, select **Specify License Server** and enter IP address or host name into the **Specify License Server** box. This is required even if the license server is running on the same machine as Dimensions RM.

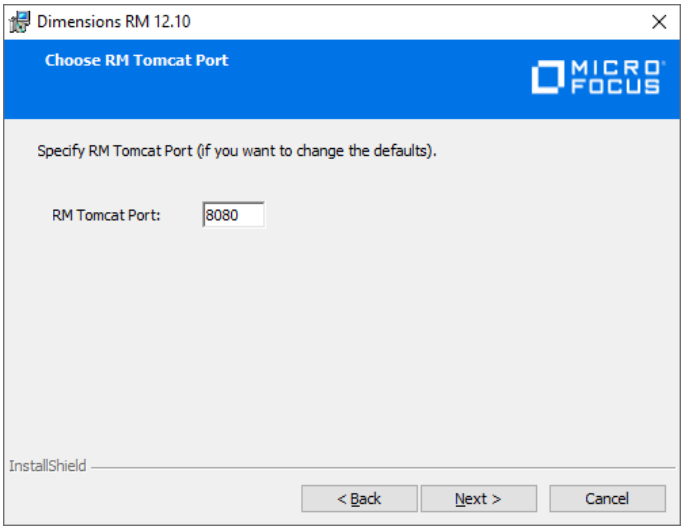
If the license tool has not yet been installed, choose **30 day evaluation**.



10 Click **Next**.

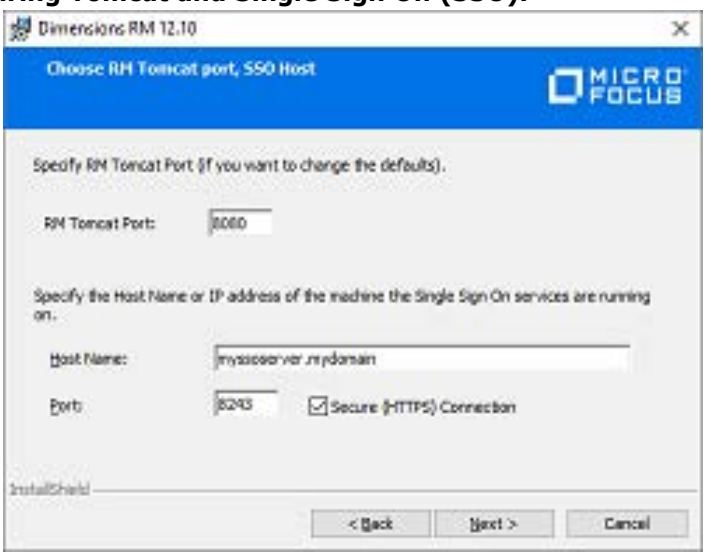
11 This dialog allows you to configure the Tomcat port. If you selected the Single Sign On (SSO) feature, this dialog also shows options for the SSO configuration.

a Configuring Tomcat only



- **RM Tomcat Port:** Specify the port under which Tomcat (and thus Dimensions RM) shall be available. The default port is **8080**. If this port is already in use, enter a different port.

b Configuring Tomcat and Single Sign On (SSO).



- **RM Tomcat Port:** Specify the port under which Tomcat (and thus Dimensions RM) shall be available. The default port is **8080**. If this port is already in use, enter a different port.
- **Host Name:** Specify the IP address or host name under which your SSO server (Dimensions CM or SBM) is available. For Windows SSO, specify the name of the machine on which you are installing Dimensions RM.
- **Port:** Specify port to be used for SSO connections.
  The default ports are 8243 (HTTPS) and 8085 (HTTP).

  Windows SSO

  When using Tomcat with HTTP, specify the Tomcat HTTP port.

  When using Tomcat with HTTPS, specify the Tomcat HTTPS port.

Secure (HTTPS) connection: Keep this option enabled to use HTTPS connections. Clear it to use unsecured (HTTP) connections.

Windows SSO

When using Tomcat with HTTP, clear the **Secure (HTTPS) Connection** option.

12 Click **Next**.

NOTE Setup now checks for a valid installation of Open Text Common Tomcat .

Installed Tomcat is a 64-bit release, all version numbers match: all web applications installed with Dimensions RM will be added to your current Tomcat installation. Proceed to Database Selection.

a Installed Tomcat is a 32-bit release

Choose from one of these options:

- **OK:** Upgrade Tomcat. This will deactivate all installed web applications. You need to copy the web applications from the `webapps` directory of the RM Installation backup to the `webapps` directory of the new Tomcat.
- **Cancel:** Exit the setup. Dimensions RM will not be installed.

b Installed Tomcat is a 64-bit release, with correct major and minor version numbers, but build and release version numbers do not match

Choose from one of these options:

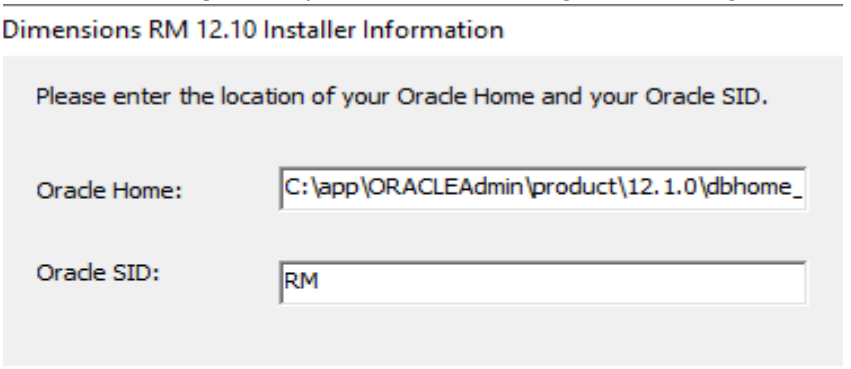
- **Yes:** Upgrade Tomcat. This will deactivate all installed web applications. You need to copy the web applications from the `webapps` directory of the RM Installation backup to the `webapps` directory of the new Tomcat.
- **No:** Continue without upgrade. This will add all web applications installed with Dimensions RM to your current Tomcat installation.
- **Cancel:** Exit the setup. Dimensions RM will not be installed.

13 Select the database and click **Next**.

- If you select **Oracle**, you will continue with step 14.
- If you select **PostgreSQL**, you will continue with step 15.
- If you select **MS SQL,** you will continue with step 17.

14 **Oracle:** Select the Oracle installation and continue with step 16.
If the list does not contain your Oracle installation, do the following

a Click **Manual Entry**. This opens the Oracle configuration dialog.



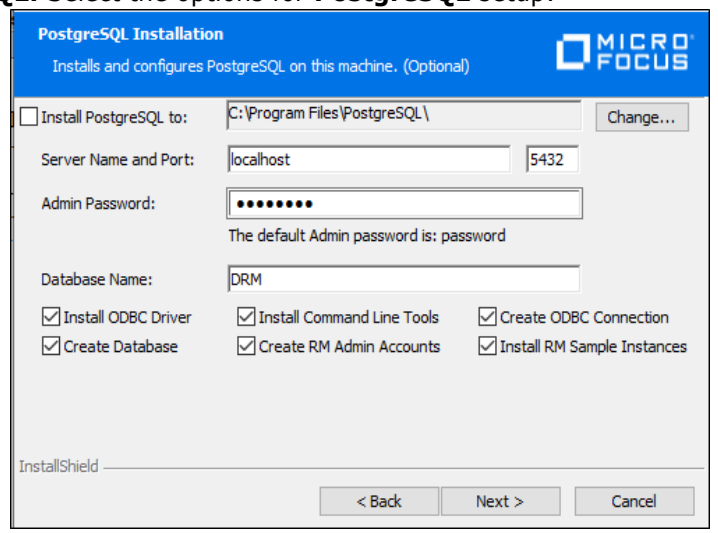
b Enter the Oracle Home path.

c Enter the Oracle SID.

d Click **OK**.

e Click **Next** and continue with step 17.

15 **PostgreSQL:** Select the options for **PostgreSQL** setup:



IMPORTANT! If the PostgreSQL is installed, and the database server is on a different machine, ensure that the database can be accessed from the machine on which Dimensions RM is installed, otherwise critical administrator functions will not work.

For details specific to PostgreSQL see chapter "Accessing PostgreSQL from other Machines" on page 151.

- **Install PostgreSQL DB to:** If this box is checked, PostgreSQL will be installed on the same machine as the Dimensions RM server in the installation directory indicated.
- Click **Change...** to select a different installation directory.

IMPORTANT! Using this simplified PostgreSQL setup, a separate path for the database files cannot be specified. If more control over the database setup is required, do the following:

- Cancel this setup.
- Start the PostgreSQL setup as described in chapter "Installing PostgreSQL" on page 148.
- Restart the Dimensions RM installation at "Run Setup.exe as Administrator" on page 54. On this pass, clear the "Install PostgreSQL DB to" checkbox.

- **Server Name:** This is the name of the server running PostgreSQL. If Dimensions RM and PostgreSQL are installed on the same machine, this **must be** `localhost`.
- **Port:** The port under which PostgreSQL is accessible. The default is 5432.
- **Admin password**: This password is used for PostgreSQL and also for the Dimensions RM accounts if you select the **Create RM Admin Accounts** and **Install RM Sample Instances** options below.
- **Database Name:** The name of the PostgreSQL database instance.
- **Install ODBC Driver:** Installs the PostgreSQL **PostgreSQL Unicode(x64)** ODBC driver that is required to access the database.
- **Create ODBC Connection:** Creates the PostgreSQL ODBC connection that is required for accessing the database. This option requires the **PostgreSQL Unicode(x64) ODBC** driver to be installed. The database name is also used as the connection name.
- **Create Database:** Creates a PostgreSQL database that is used to receive the Dimensions RM data.
- **Create RM Admin Accounts:** Creates the `ICDBA` and `ICADMIN` accounts and assigns them the admin password.
- **Install RM Sample Instances:** Installs the Dimensions RM instances. For security reasons, it is recommended to use this option on **non-production** systems only.

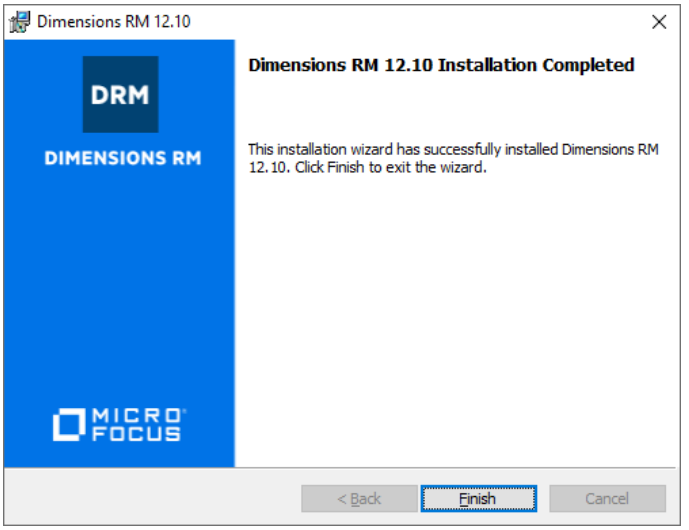
16 Click **Next**.

17 Enter the path to the `security.dat` file. This file must be stored under RM in the installation directory tree, for example:
`C:\Program Files\Open Text\Dimensions 12.11.2 (23.4)\RM\security.dat`

18 If you want to see shortcuts for the client applications on the server desktop, select the **Add Shortcuts** box.

19 Click **Install** to start the installation process.

20 Once the *Successfully Completed* install dialog is raised, click **Finish**.



21 If you are upgrading your installed version of Dimensions RM, please continue with the process: Chapter 2, "Post-Upgrade Tasks" on page 27.

22 If this is a fresh installation, please continue with the process: Chapter 3, "Post-Installation Tasks" on page 37

Running Setup.exe without Internet Connection

In general, there is no difference if you run setup.exe in an environment with or without Internet connection.

However, as Setup.exe is digitally signed, it can only run if the digital signature can be verified. Should the verification fail, you may receive the following error message:

```
Error 1330. A file that is required cannot be installed because the
    cabinet file <FILE_PATH>\Data1.cab has an invalid digital
    signature. This may indicate that the cabinet file is corrupt.
    Error 266 was returned by WinVerifyTrust.
```

In this case, do the following:

1 Exit the running Setup.exe.

2 Open a command prompt.

3 Type `mmc` and press **Enter**. This opens a console window.

4 From the **File** menu, select **Add/Remove Snap-in**. This opens the **Add or Remove Snap-ins** dialog.

5 Select **Certificates** and click **Add**. This opens the **Certificates snap-in** dialog.

6 Select the **Computer account** option and click **Next**.

7 Ensure that option **Local computer: (the computer the console is running on)** is selected and click **Finish**.

8 Click **OK**.

9 Expand **Certificates (Local Computer)**.

10 Expand **Trusted Root Certification Authorities**.

11 Right-click **Certificates** and select **All Tasks** and then **Import...** from the shortcut menu. This opens the **Certificate Import Wizard**.

12 Click **Next**.

13 Click **Browse...**. This opens a file selection dialog.

14 Navigate to the folder where Setup.exe is located.

15 Navigate to the sub-folder **support**.

16 Select the certificate `Entrust_Root_Certification_Authority_G2.cer` and click **Open**.

17 Click **Next**.

18 Verify that the **Place all certificates in the following store** option is selected and the **Certificate store** box shows **Trusted Root Certification Authorities**.
If the verification fails, click **Cancel** and return to point 10.

19 Click **Next**.

20 Click **Finish** to import the certificate

21 Confirm the success message by clicking **OK**.

Chapter 6

Related Activities

Installation Related Activities

This chapter discusses the installation related procedures and checks that are important to a healthy relationship with Dimensions RM, but not necessary to a functioning installation.

IMPORTANT! When using RM Manage from a client machine, changes will not take effect until the **Open Text Dimensions RM Pool Manager** service is restarted on the RM server.

Virus Checkers

Real-time virus checking of certain Dimensions RM and database files can cause a noticeable slowdown in the Dimensions RM server operations. The following list identifies the principal files that can be excluded from real-time virus to improve performance:

IMPORTANT! The files listed below should, of course, still be included in other forms of virus scans—it is only their exclusion from real-time checking for all reads and writes during operation that is being recommended.

File Name	Execution Mode	Risks Introduced by Excluded from Real-Time Virus Checking
Datacacheserver.exe	■ Run as system user continuously once the product is installed. ■ Memory usage of this particular process increases/decreases depending upon the load. ■ Multiple process are launched and run in the memory.	This executable is continuously using the active system memory and is accessed by each and every request over the Internet or intranet.
rmAppserver.exe	■ Run as system user continuously once the product is installed. ■ Memory usage of this particular process increases/decreases depending upon the load. ■ Multiple process are launched and run in the memory.	As above.

File Name	Execution Mode	Risks Introduced by Excluded from Real-Time Virus Checking
RMServerPool.exe	■ Run as system user continuously once the product is installed. ■ Memory usage of this particular process increases/decreases depending upon the load. ■ Multiple process are launched and run in the memory.	As above.
Oracle, PostgreSQL, or MS sqlserver executables	■ Run as established system user continuously once the product is started. ■ Memory usage of this particular process increases/decreases depending upon the load.	As above.

Running Dimensions RM with Limited Permissions

IMPORTANT!

When running Dimensions RM with limited permissions:

- importing of MS Word documents in RM Browser is not supported
- importing of MS Word documents using RM Import is only supported on client machines.

To run Dimensions RM with limited permissions, perform the following tasks, located in order in the following sections:

- It is recommended to create a local standard user account if it does not already exist (see chapter"Creating a Local Standard User Account" on page 66).
- Set the folder permissions as described in chapter "Setting Folder Permissions" on page 67.
- Set the registry permissions as described in chapter "Setting Registry Key Permissions" on page 68.

- Configure RM License Agent as described in chapter "Configuring the RM License Agent for Limited Permissions" on page 70.
- Remove "Word Document" from RM's "Import" menu as described in chapter "Removing "Word Document" from RM's "Import" menu" on page 71
- If Microsoft Word is installed, execute the steps as described in chapter "Using Microsoft Office on Windows Server with Limited Permissions" on page 73.
- Configure the Dimensions RM services as described in chapter "Running Dimensions RM Services with Limited Permissions" on page 72.

Creating a Local Standard User Account

To allow Dimensions RM using Microsoft Word, Microsoft Word needs to run under a local administrator account. It is suggested to use a separate account with a user name which identifies its function.

To create a local standard user account, follow these steps:

1. Open Windows Control Panel.
2. In Category view, select **Large icons** or **Small icons**.
3. Click **Administrative Tools**.
4. Start **Computer Management**.
5. Expand **System Tools**.
6. Expand **Local Users and Groups**.
7. Right-click **Users** and select **New User...** from the shortcut menu. This opens the **New User** dialog.
8. In the **User name** box, enter the account name you want to create, e.g. `RMServiceUser`.
9. In the **Password** box, enter a complex password.
10. Repeat the password in the **Confirm password** box.
11. Take a note of that password.
12. Ensure that the **User must change password at next logon** box is clear.
13. Select the **User cannot change password** box.
14. Select the **Password never expires** box.
15. Click **Create**.
16. Click **Close**.

PRIVILEGES To prevent local or remote login, see chapter "Preventing Local and Remote Login for a User Account" on page 76.

Setting Folder Permissions

Execute the following steps to set folder permissions:

1. Navigate to your *RM_Install*\RM directory, e.g. *C:\Program Files\Dimensions 12.11.2 (23.4)\RM*.
2. Right-click the logs folder and select Properties from the shortcut menu. This opens the **logs Properties** dialog.
3. Select the **Security** tab.
4. Click **Advanced**. This opens the **Advanced Security Settings** dialog.
5. Click **Add**. This opens the **Permission Entry** dialog.
6. Click **Select a principal**. This opens the **Select User or Group** dialog.
7. Enter the user name into the **Enter the object name to select box** and click **Check Names**. This completes the user name and underlines it.
8. Click **OK**.
9. Click **Show advanced permissions**.
10. Ensure that the following permissions are selected:
    - Traverse folder / execute file
    - List folder / read data
    - Read attributes
    - Read extended attributes
    - Create files / write data
    - Create folders / append data
    - Write attributes
    - Write extended attributes
    - Delete subfolders and files
    - Read permissions
11. Click **OK**.
12. Select the **Replace all child object permission entries with inheritable permission entries from this object** option.
13. Click **OK**.
14. Navigate to your *RM_Install*\RM\conf directory, e.g. *C:\Program Files\Dimensions 12.11.2 (23.4)\RM*\conf.
15. Right-click the autopass folder and select Properties from the shortcut menu. This opens the **autopass Properties** dialog.
16. Select the **Security** tab.

17 Click **Advanced**. This opens the **Advanced Security Settings** dialog.

18 Click **Add**. This opens the **Permission Entry** dialog.

19 Click **Select a principal**. This opens the **Select User or Group** dialog.

20 Enter the user name into the **Enter the object name to select box** and click **Check Names**. This completes the user name and underlines it.

21 Click **OK**.

22 Click **Show advanced permissions**.

23 Ensure that the following permissions are selected:

- Traverse folder / execute file
- List folder / read data
- Read attributes
- Read extended attributes
- Create files / write data
- Create folders / append data
- Write attributes
- Write extended attributes
- Delete subfolders and files
- Read permissions

24 Click **OK**.

25 Select the **Replace all child object permission entries with inheritable permission entries from this object** option.

26 Click **OK**.

27 Navigate to your Tomcat root directory, e.g. *C:\Program Files\Dimensions 12.11.2 (23.4)\Common Tools 1.8.6.0\tomcat\9.0.*

28 Right-click the `logs` folder and repeat steps 3 - 13.

29 Right-click the `temp` folder and repeat steps 3 - 13.

30 Right-click the `work` folder and repeat steps 3 - 13.

31 Navigate to the `webapps` folder.

32 Navigate to the `rtmBrowser` folder.

33 Right-click the `temp` folder and repeat steps 3 - 13.

Setting Registry Key Permissions

To set registry key permissions, execute the following steps:

1. Start the Windows Registry Editor (regedit.exe).
2. Expand `HKEY_LOCAL_MACHINE\SOFTWARE`.
3. If the key `Hewlett-Packard` does not exist, create it by executing the following steps:
   a. Right-click the `SOFTWARE` key. This opens the shortcut menu.
   b. Point to **New** and select **Key**. This creates a new key with a name like *New Key #1* ready for changing the name.
   c. Type `Hewlett-Packard` and press **Enter**.
4. Right-click the `Hewlett-Packard` key and select **Permissions...** to open the **Permissions for Hewlett-Packard** dialog.
5. Click **Add...** to open the **Select Users or Group** dialog.
6. Enter the user name you created in chapter "Creating a Local Standard User Account" on page 66 (e.g. *`RMServiceUser`*) into the **Enter the object name to select box** and click **Check Names**. This completes the user name and underlines it.
7. Click **OK**.
8. Ensure that the user you added is selected.
9. Select the following options:
   - Full Control
   - Read
10. Click **OK**.
11. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\JavaSoft` and expand it.
12. Right-click the `Prefs` key and select **Permissions...** to open the **Permissions for Prefs** dialog.
13. Click **Add...** to open the **Select Users or Group** dialog.
14. Enter the user name you created in chapter "Creating a Local Standard User Account" on page 66 (e.g. *`RMServiceUser`*) into the **Enter the object name to select box** and click **Check Names**. This completes the user name and underlines it.
15. Click **OK**.
16. Ensure that the user you added is selected.
17. Select the following options:
    - Full Control
    - Read
18. Click **OK**.
19. Navigate to `"HKEY_LOCAL_MACHINE\SOFTWARE\Open Text"` and expand it.
20. Right-click the `Dimensions RM` key and select **Permissions...** to open the **Permissions for Dimensions RM** dialog.
21. Click **Add...** to open the **Select Users or Group** dialog.

22 Enter the user name you created in chapter "Creating a Local Standard User Account" on page 66 (e.g. *RMServiceUser*) into the **Enter the object name to select box** and click **Check Names**. This completes the user name and underlines it.

23 Click **OK**.

24 Ensure that the user you added is selected.

25 Select the following options:

- Full Control
- Read

26 Click **OK**.

Configuring the RM License Agent for Limited Permissions

This chapter configures RM License Agent to allow Dimensions RM running with limited permissions.

To configure RM License Agent for limited permissions, execute the following steps:

1 Ensure that you prepared the server as described in chapter "Creating a Local Standard User Account" on page 66.

2 Open the command prompt and type one of the following commands and press **Enter**: `comexp.msc`

3 Navigate to `Component Services | Computers | My Computer | DCOM Config`

4 Right-click **RM License Agent** and select **Properties**.

5 Select the **Security** tab.

6 In the **Launch and Activation Permissions** section, select **Customize**.

7 Click **Edit...** to open the **Launch and Activation Permission** dialog.

8 Click **Add...** to open the **Select Users or Groups** dialog.

9 Enter the user name you created in chapter "Creating a Local Standard User Account" on page 66 (e.g. *RMServiceUser*) into the **Enter the object name to select box** and click **Check Names**. This completes the user name and underlines it.

10 Click **OK**.

11 Ensure that the following options are selected:

- Local Launch
- Local Activation

12 Click **OK** to close the **Launch and Activation Permission** dialog.

13 In the **Access Permissions** section, select **Customize**.

14 Click **Edit...** to open the **Access Permissions** dialog.

15 Click **Add...** to open the **Select Users or Groups** dialog.

16 Enter the user name (e.g. *RMServiceUser*) into the **Enter the object name to select box** and click **Check Names**. This completes the user name and underlines it.

17 Click **OK**.

18 Ensure that the following options are selected:

- Local Access
- Remote Access

19 Click **OK** to close the **Access Permissions** dialog.

20 In the **Configuration Permissions** section, select **Customize**.

21 Click **Edit...** to open the **Change Configuration Permissions** dialog.

22 Click **Add...** to open the **Select Users or Groups** dialog.

23 Enter the user name you created in chapter "Creating a Local Standard User Account" on page 66 (e.g. *RMServiceUser*) into the **Enter the object name to select box** and click **Check Names**. This completes the user name and underlines it.

24 Click **OK**.

25 Ensure that the following options are selected:

- Full Control
- Read

26 Click **OK** to close the **Change Configuration Permissions** dialog.

27 Select the **Identity** tab.

28 Select the **This user** option.

29 Click **Browse...** to open the **Select User** dialog.

30 Enter the user name you created in chapter "Creating a Local Standard User Account" on page 66 (e.g. *RMServiceUser*) into the **Enter the object name to select box** and click **Check Names**. This completes the user name and underlines it.

31 Click **OK**.

32 In the **Password** box, enter a the password for the selected user.

33 Repeat the password in the **Confirm password** box.

34 Click **OK** to close the **RM License Agent Properties** dialog.

Removing "Word Document" from RM's "Import" menu

When running Dimensions RM with limited permissions, importing Microsoft Word documents is not supported. Note that this also includes Roundtrip documents as these are Microsoft Word documents.

To remove "Word Document" from the "Import" menu, do the following:

1. Navigate to ***RM_INSTALL***\Common Tools 2.3.0.0\tomcat\9.0\webapps\rtmBrowser\rm\frame\panels\top, e.g. *C:\Program Files\Open Text\Dimensions 12.11.2\Common Tools 2.3.0.0\tomcat\9.0\webapps\rtmBrowser\rm\frame\panels\top*.
2. Open the file `toppanel.jsp` with a text editor, e.g. Notepad.
3. Search for **RM_TopPanel_ImportFromWordDocument**.
4. Surround the parent item with <%-- and --%>, so it looks like this:

```
<%-- <sct:subMenuItem
href="javascript:SERENA.rm.panels.top.showImportWordDocumentDialog()
">

<fmt:message key="RM_TopPanel_ImportFromWordDocument" />

</sct:subMenuItem> --%>
```

5. Save the file.
6. Restart the **Open Text Common Tomcat** service.

Running Dimensions RM Services with Limited Permissions

To run Dimensions RM services with limited permissions, execute these steps:

1. Ensure that you executed the previous configuration steps as described in these chapters:
   - "Creating a Local Standard User Account" on page 66
   - "Setting Folder Permissions" on page 67
   - "Configuring the RM License Agent for Limited Permissions" on page 70
   - "Removing "Word Document" from RM's "Import" menu" on page 71
2. In a command prompt, type `services.msc` and press **Enter**.
3. From the list, select the **Open Text Common Tomcat** service and click **Stop**.
4. Double-click the **Open Text Common Tomcat** service.
5. Select the **Log On** tab.
6. Select the **This account** option.
7. Enter user name and password. For the user name, use the user you created in chapter "Creating a Local Standard User Account" on page 66, e.g. *RMServiceUser*.
8. From the list, select the **Open Text Common Tomcat** service and click **Start**.
9. From the list, select the **Open Text Dimensions RM Pool Manager** service and click **Stop**.
10. Double-click the **Open Text Dimensions RM Pool Manager** service.
11. Select the **Log On** tab.

12 Select the **This account** option.

13 Enter user name and password. For the user name, use the user you created in chapter "Creating a Local Standard User Account" on page 66, e.g. *RMServiceUser*.

14 Click **OK**.

Using Microsoft Office on Windows Server with Limited Permissions

This chapter configures Windows Server to allow using Microsoft Office when Dimensions RM runs with limited permissions. This means that Microsoft Office can be used for export.

IMPORTANT! When running Dimensions RM with limited permissions, importing of MS Word documents is not supported.

To allow Dimensions RM to use Microsoft Office with limited permissions, execute the following steps:

1 Ensure that you prepared the server as described in chapter "Running Dimensions RM with Limited Permissions" on page 65.

2 Open the command prompt and type one of the following commands and press **Enter**:

- For Microsoft Office 32-bit: `comexp.msc /32`
- For Microsoft Office 64-bit: `comexp.msc`

3 Navigate to `Component Services | Computers | My Computer | DCOM Config`

4 Right-click **Microsoft Excel Application** and select **Properties**.

5 Select the **Security** tab.

6 In the **Launch and Activation Permissions** section, select **Customize**.

7 Click **Edit...** to open the **Launch and Activation Permission** dialog.

8 Click **Add...** to open the **Select Users or Groups** dialog.

9 Enter the user name you created in chapter "Creating a Local Standard User Account" on page 66 (e.g. *`RMServiceUser`*) into the **Enter the object name to select box** and click **Check Names**. This completes the user name and underlines it.

10 Click **OK**.

11 Ensure that the following options are selected:

- Local Launch
- Local Activation

12 Click **OK** to close the **Launch and Activation Permission** dialog.

13 Select the **Identity** tab.

14 Select the **This user** option.

15 Click **Browse...** to open the **Select User** dialog.

16 Enter the user name you created in chapter "Creating a Local Standard User Account" on page 66 (e.g. *RMServiceUser*) into the **Enter the object name to select box** and click **Check Names**. This completes the user name and underlines it.

17 Click **OK**.

18 In the **Password** box, enter a the password for the selected user.

19 Repeat the password in the **Confirm password** box.

20 Click **OK** to close the **Microsoft Excel Application Properties** dialog.

21 Right-click **Microsoft PowerPoint Slide** and select **Properties**.

22 Select the **Security** tab.

23 In the **Launch and Activation Permissions** section, select **Customize**.

24 Click **Edit...** to open the **Launch and Activation Permission** dialog.

25 Click **Add...** to open the **Select Users or Groups** dialog.

26 Enter the user name you created in chapter "Creating a Local Standard User Account" on page 66 (e.g. *RMServiceUser*) into the **Enter the object name to select box** and click **Check Names**. This completes the user name and underlines it.

27 Click **OK**.

28 Ensure that the following options are selected:

- Local Launch
- Local Activation

29 Click **OK** to close the **Launch and Activation Permission** dialog.

30 Select the **Identity** tab.

31 Select the **This user** option.

32 Click **Browse...** to open the **Select User** dialog.

33 Enter the user name you created in chapter "Creating a Local Standard User Account" on page 66 (e.g. *RMServiceUser*) into the **Enter the object name to select box** and click **Check Names**. This completes the user name and underlines it.

34 Click **OK**.

35 In the **Password** box, enter a the password for the selected user.

36 Repeat the password in the **Confirm password** box.

37 Click **OK** to close the **Microsoft PowerPoint Slide Properties** dialog.

38 Right-click **Microsoft Word 97 - 2003 Document**, **Microsoft Word Document** or **Microsoft Office Word Document** and select **Properties**.

39 Select the **Security** tab.

40 In the **Launch and Activation Permissions** section, select **Customize**.

41 Click **Edit...** to open the **Launch and Activation Permission** dialog.

42 Click **Add...** to open the **Select Users or Groups** dialog.

43 Enter the user name you created in chapter "Creating a Local Standard User Account" on page 66 (e.g. *RMServiceUser*) into the **Enter the object name to select box** and click **Check Names**. This completes the user name and underlines it.

44 Click **OK**.

45 Ensure that the following options are selected:

- Local Launch
- Local Activation

46 Click **OK** to close the **Launch and Activation Permission** dialog.

47 In the **Access Permissions** section, select **Customize**.

48 Click **Edit...** to open the **Access Permissions** dialog.

49 Click **Add...** to open the **Select Users or Groups** dialog.

50 Enter the user name you created in chapter "Creating a Local Standard User Account" on page 66 (e.g. *RMServiceUser*) into the **Enter the object name to select box** and click **Check Names**. This completes the user name and underlines it.

51 Click **OK**.

52 Ensure that the following options are selected:

- Local Access
- Remote Access

53 Click **OK** to close the **Access Permissions** dialog.

54 In the **Configuration Permissions** section, select **Customize**.

55 Click **Edit...** to open the **Change Configuration Permissions** dialog.

56 Click **Add...** to open the **Select Users or Groups** dialog.

57 Enter the user name you created in chapter "Creating a Local Standard User Account" on page 66 (e.g. *RMServiceUser*) into the **Enter the object name to select box** and click **Check Names**. This completes the user name and underlines it.

58 Click **OK**.

59 Ensure that the following options are selected:

- Full Control
- Read

60 Click **OK** to close the **Change Configuration Permissions** dialog.

61 Select the **Identity** tab.

62 Select the **This user** option.

63 Click **Browse...** to open the **Select User** dialog.

64 Enter the user name you created in chapter "Creating a Local Standard User Account" on page 66 (e.g. *RMServiceUser*) into the **Enter the object name to select box** and click **Check Names**. This completes the user name and underlines it.

65 Click **OK**.

66 In the **Password** box, enter a the password for the selected user.

67 Repeat the password in the **Confirm password** box.

68 Click **OK** to close the **Properties** dialog.

69 In a command prompt, type `services.msc` and press **Enter**.

70 Restart the **Open Text Dimensions RM Pool Manager** service.

Preventing Local and Remote Login for a User Account

To prevent local or remote login, follow these steps:

1 From the Start menu, select `Administrative Tools | Local Security Policy` or open the **Control Panel** in Icon view and click **Administrative Tools**. This opens the **Local Security Policy** dialog.

2 In the **Local Security Policy** dialog, expand **Local Policies**.

3 Select **User Rights Assignment**.

4 Double-click **Deny log on locally**.

5 Click **Add User or Group...**

6 Type *RMServiceUser* into the **Enter the object names to select (examples)** box and click **Check Names**. This should show SERVER_NAME*RMServiceUser*.

7 Click **OK**.

8 Click **OK**.

9 Double-click **Deny log on through Remote Desktop Services**.

10 Click **Add User or Group...**

11 Type *RMServiceUser* into the **Enter the object names to select (examples)** box and click **Check Names**. This should show SERVER_NAME*RMServiceUser*.

12 Click **OK**.

13 Click **OK**.

Support for Export/Import

Dimensions RM provides export functions to Word, Excel, and PowerPoint as well as import functions for Word, and Excel. In order to provide these functionalities,

Dimensions RM needs to access Microsoft Office (32-bit or 64-bit). After running the Dimensions RM setup, do the following:

1 Ensure that the following paths exist:

- `C:\Windows\System32\config\systemprofile\Desktop`
- `C:\Windows\SysWOW64\config\systemprofile\Desktop`
- `C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Windows\INetCache`
- `C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\INetCache`

2 Choose one of these following configurations:

- To run Dimensions RM will full permissions (requires local administrator account; allows import and export), execute the steps described in chapter "Running Dimensions RM with Full Permissions" on page 77.
- To run Dimensions RM with limited permissions (requires local standard user account; allows export only), execute the steps described in chapter "Running Dimensions RM with Limited Permissions" on page 65.

3 When using Adobe Reader on the server, execute the steps described in chapter "Using Adobe Reader on Windows Server" on page 81.

Running Dimensions RM with Full Permissions

To run Dimensions RM with full permissions, do the following:

- It is recommended to create a local administrator account if it does not already exist (see chapter"Creating a Local Administrator Account" on page 77).
  If you can't create a local administrator account, e.g. due to regulations, skip this step.
- Configure the **Open Text Dimensions RM Pool Manager** service as described in chapter "Using Microsoft Office on Windows Server with Full Permissions" on page 79.
- If you are using a local administrator account, prepare the server for PDF Import (see chapter "Preparing for PDF Import on Windows Server" on page 81).

Creating a Local Administrator Account

To allow Dimensions RM using Microsoft Word, Microsoft Word needs to run under a local administrator account. It is suggested to use a separate account with a user name which identifies its function.

To create a local Administrator account, follow these steps:

1 Open Windows Control Panel.

2 In Category view, select **Large icons** or **Small icons**.

3 Click **Administrative Tools**.

4 Start **Computer Management**.

5 Expand **System Tools**.

6 Expand **Local Users and Groups**.

7 Right-click **Users** and select **New User...** from the shortcut menu. This opens the **New User** dialog.

8 In the **User name** box, enter the account name you want to create, e.g. `RMServiceUser`.

9 In the **Password** box, enter a complex password.

10 Repeat the password in the **Confirm password** box.

11 Take a note of that password.

12 Ensure that the **User must change password at next logon** box is clear.

13 Select the **User cannot change password** box.

14 Select the **Password never expires** box.

15 Click **Create**.

16 Click **Close**.

17 Select the **Administrator** option.

18 Click **Finish**.

19 In the tree, select **Users**. This shows a list of users.

20 Right-click user *RMServiceUser* and select **Properties** from the shortcut menu. This opens the *RMServiceUser* **Properties** dialog.

21 Select the **Member Of** tab.

22 Click **Add...**

23 Type `Administrators` into the **Enter the object names to select (examples)** box and click **Check Names**. This should show SERVER_NAME\Administrators.

24 Click **OK**.

25 Click **OK**.

26 Change to the log on page and log on with user *RMServiceUser*.

27 Start Microsoft Word and confirm any dialogs.

28 Open a PDF file in Microsoft Word. This will open a message box with a warning that the layout may not be identical.

29 Set the **Don't show this message again** option and click **OK**.

30 Start any other installed Microsoft Office application and confirm any dialogs.

31 Log off user *RMServiceUser*.

32 Log in with your Administrator account to continue with the next steps.

PRIVILEGES To prevent local or remote login, see chapter "Preventing Local and Remote Login for a User Account" on page 76.

Using Microsoft Office on Windows Server with Full Permissions

This chapter configures Windows Server to allow Dimensions RM running with full permissions, which ensures Microsoft Office can be used for export and import.

To allow Dimensions RM to use Microsoft Office with full permissions, execute the following steps:

1 Ensure that you prepared the server as described in chapter"Creating a Local Administrator Account" on page 77.

2 Open the command prompt.

3 Type `services.msc` and press **Enter**.

4 From the list, select the **Open Text Dimensions RM Pool Manager** service and click **Stop**.

5 Double-click the **Open Text Dimensions RM Pool Manager** service.

6 Select the **Log On** tab.

7 If you created a local administrator account (suggested), do this:

a Select the **This account** option.

b Enter user name and password. For the user name, use the user you created in chapter "Creating a Local Administrator Account" on page 77.

8 If you can’t create a local administrator account, e.g. due to regulations, do this:

a Ensure that the **Local System account** option is selected.

b Ensure that the **Allow service to interact with desktop** option is selected.

NOTE If you do not create a local administrator account and configure Dimensions RM as described in the related steps, PDF import will not work and the related process will not continue. To avoid users using the .PDF file filter on the Word import dialog, do the following:

a Navigate to ***RM_INSTALL***`\Common Tools 1.8.6.0\tomcat\9.0\webapps\rtmBrowser\rm\import`

b Open `icWebWordImport.js` with a text editor, e.g. Notepad.

c Locate the line `var extArray = new Array(".doc", ".docx", ".pdf");`

d Remove the filter for the PDF file extension, so it looks like this:

```
var extArray = new Array(".doc", ".docx");
```

e Save the file.

Note that the above changes does not completely prevent the attempt to import PDF files as users may select the PDF file by using the *.* file filter.

9 Click **OK**.

10 From the list, select the **Open Text Dimensions RM Pool Manager** service and click **Start**.

For Microsoft Office 32-bit:

1 Open a command prompt.

2 Type `comexp.msc /32` and press **Enter**. This opens the **Component Services** dialog.

3 Navigate to `Component Services | Computers | My Computer | DCOM Config`

4 Right-click **Microsoft Word 97 - 2003 Document**, **Microsoft Word Document** or **Microsoft Office Word Document** and select **Properties**.

5 Select the **Identity** tab.

6 Select **The launching user.**

7 Click **OK**.

For Microsoft Office 64-bit:

1 Open a command prompt.

2 Type `comexp.msc` and press **Enter**. This opens the **Component Services** dialog.

3 Navigate to `Component Services | Computers | My Computer | DCOM Config`

4 Right-click **Microsoft Word 97 - 2003 Document**, **Microsoft Word Document** or **Microsoft Office Word Document** and select **Properties**.

5 Select the **Identity** tab.

6 Select **The launching user.**

7 Click **OK**.

Preparing for PDF Import on Windows Server

With RM release 12.8, PDF documents can be imported. To ensure that PDF documents can be processed, it is essential that the server is prepared accordingly.

To prepare the server for PDF document import, follow these steps:

1. Log on with user who is configured for the RM Pool Manager service. If you followed the suggested name, the user name is *RMServiceUser*.
2. Open a PDF file in Microsoft Word. This will open a message box with a warning that the layout may not be identical.
3. Set the **Don't show this message again** option and click **OK**.

Using Adobe Reader on Windows Server

If Adobe Reader is installed on the server, exporting documents can cause RM Browser to hang. This occurs if the document you export contains a PDF document (e.g. through a file attachment of a requirement). Execute the following steps to allow the SYSTEM user account to access Adobe Reader:

1. Open a command prompt.
2. Type `comexp.msc /32` and press Enter.
3. Navigate to `Component Services | Computers | My Computer | DCOM Config`
4. Right-click **Adobe Acrobat Document** and select **Properties**.
5. Select the **Identity** tab.
6. Select **The interactive user**.
7. Click **OK**.

Configuring Windows SSO

Skip this section if you do not want to use **Windows SSO**, i.e. you do not use SSO or use SSO with Solutions Business Manager (SBM) or Dimensions CM.

Windows SSO has been reconfigured to use the Waffle Library; there is no longer a zip file included with the release.

If, in a previous release, you have configured Dimensions RM to use Windows SSO, the following instructions will allow you to continue to use Windows SSO in this release.

If this is a new Dimensions RM Installation, or if you are preparing to use Windows SSO for the first time, please contact support: http://supportline.microfocus.com

To re-configure Windows SSO, do the following:

1. Stop **Open Text Common Tomcat** Service.
2. Stop the **RM Pool Manager** service.
3. In Windows Explorer, navigate to ***tomcat\9.0\conf***, e.g.
   e.g., "C:\Program Files\Open Text\Dimensions 12.11.2\Common Tools 2.3.0.0\tomcat\9.0\conf".
4. Locate web.xml, open the file for editing.
   change the **gatekeeper.enabled** parameter to false:
   ```
   <init-param>
   <param-name>gatekeeper.enabled</param-name>
   <param-value>false</param-value>
   </init-param>
   ```
5. In Windows Explorer, navigate to **tomcat\9.0\webapps**
   "C:\Program Files\Open Text\Dimensions 12.11.2\Common Tools 2.3.0.0\tomcat\9.0\webapps".

   Delete idp.war and idp folder
6. In Windows Explorer, navigate to **tomcat\9.0\webapps\rtmBrowser\WEB-INF**
   "C:\Program Files\Open Text\Dimensions 12.11.2\Common Tools 2.3.0.0\tomcat\9.0\webapps\rtmBrowser\WEB-INF"
7. Locate web.xml, open the file for editing.
   enable the **WinSSOFilter** filter:
   ```
   <filter-name>WinSSOFilter</filter-name>
   <filter-class>de.qp.rm.sso.WinSSOFilter</filter-class>
   <init-param>
   <param-name>enabled</param-name>
   <param-value>true</param-value>
   </init-param>
   ```
8. Go to **RM Manage** -> Login sources. (see Configuring Login Sources in the *Administrator's Guide*)
   Enable LDAP and turn off SBM SSO login source**.**
9. In **RM Manage** -> Go to the Configuration tab and set values for the LDAP server.
10. Enable Auto Create Users and assign default group and category (see Creating Users Automatically in the *Administrator's Guide*)
11. Kill all running RM License Tool processes in Task Manager.
12. Start the following services:
    - RM Pool Manager
    - Micro Focus Common Tomcat
13. Try logging in with RM Browser

If you have issues, please contact support: http://supportline.microfocus.com. Include details and, if possible, screen shots describing the issue.

The ICDBA Account

Before you can log in to Dimensions RM, you have to create an ICDBA database account and password in the database instance that is to be used for Dimensions RM.

There are two methods of doing this:

- Using RM Manage "Create ICDBA Account" (Recommended)

  For further details, see chapter "Creating the ICDBA Account From Within RM Manage" on page 83.

- Creating the ICDBA account through a database script:
  - **Oracle:** See chapter "Oracle: Creating the ICDBA Account by Script" on page 84
  - **SQL Server:** See chapter "SQL Server: Creating the ICDBA Account by Script" on page 85

Creating the ICDBA Account From Within RM Manage

To create the ICDBA account:

1. Select the database in which you want to create the ICDBA account, e.g. *RM*.
2. To open the **Create ICDBA account** dialog, do one of the following:
   - From the **File** menu, select **Create ICDBA Account**;

     or

   - Right-click the database and select **Create ICDBA Account** from the shortcut menu.
3. Specify the ICDBA password in the **Create ICDBA account** section:
   a. In the **Password** field, type the password that you want to assign to the Dimensions RM ICDBA account.
   b. In the associated **Confirm Password** field, re-type the password.
4. Specify `SYSDBA` user name and password in the **Enter SYSDBA account password** section:
   a. In the **Account Name** field, enter the appropriate `SYSDBA` account that you want to use. The following account names are the RDBMS defaults:
      - **Oracle:** `SYS`
      - **MS SQL Server:** `sa`

   b. In the associated **Password** field, type the associated password for the `SYSDBA` account name.
5. By default, the ICDBA account is created in a new `SERENA_RM_ADMIN` tablespace for the ICDBA account and its size is set to 1024 MB. To set a different size or create the ICDBA account in an existing tablespace, click the **Advanced** button. The dialog expands to display the advanced features.
   - To set a different size for the `SERENA_RM_ADMIN` tablespace, set the **Tablespace** and **Units** values as desired.

- To create the ICDBA account in an existing tablespace, select the **Create in existing tablespace** option, and select the desired tablespace from the list.
- If you wish to resize one of the tablespaces or create a new one with a specific name, click the **Administer Tablespaces** button and complete the fields as necessary.

6 Click **Create**.

IMPORTANT! Oracle Password Expiration

By default, Oracle account passwords expire after 180 days. Unless your DBA has re-configured such RDBMS to override this default and allow permanent passwords, you must change the ICDBA password before 180 days elapse using RM Manage. For details, see *"Database Administrator Accounts: Changing Passwords and Unlocking"* in the *Administrator's Guide*.

Oracle: Creating the ICDBA Account by Script

Follow these steps to create the ICDBA account:

1 Open a Windows command prompt window as administrator.

2 Navigate to ***RM_Install***`\RM\sql\oracle`
(e.g. C:\Program Files\Open Text\Dimensions 12.11.2 (23.4)\RM\sql\oracle).

3 Type `notepad create_icdba.sql` and press **Enter**.

4 Replace **change_me** with the desired password for the ICDBA user account.

5 Save the file and close notepad.

6 In the command prompt, type `sqlplus` and press **Enter**.

7 For the user name, enter the following and press Enter: `sys@`*DBNAME* `as sysdba`
Replace *DBNAME* with the name of your database, e.g. ORCL.

8 Type the password and press **Enter**. Note that when the password, no characters are shown on the screen).

9 Type `@create_icdba.sql` and press **Enter**.

10 After the user account has been created, type `exit` and press **Enter**. This terminates SQLPlus.

11 Type the following (all on one line) and press **Enter**:
`..\..\bin\icManage.exe cmd_install_icdba -location` *DBNAME*
`-icdba_password` *password*
Replace *DBNAME* with the name of your database, e.g. ORCL.
Replace *password* with the password you specified in point 4.

12 For security purposes, it is recommended to change the password in the create_icdba.sql file back to change me by executing these steps:

a In the command prompt, type `notepad create_icdba.sql` and press **Enter.**

b Replace the password for the ICDBA user account to **change_me**.

c Save the file and close notepad.

SQL Server: Creating the ICDBA Account by Script

Follow these steps to create the ICDBA account:

1. Start SQL Server Management Studio.
2. **Server type:** Select **Database Engine**.
3. **Server name:** If SQL Server is on a different machine, enter the server name or IP address of the server running SQL Server.
4. **Authentication**: Select **SQL Server Authentication**.
5. **Log in:** Type **sa**.
6. **Password:** Type the password for the **sa** user account.
7. Click **Connect**.
8. If required, expand the root node in Object Explorer.
9. Change to the Windows desktop and open Windows Explorer.
10. In Windows Explorer, navigate to *RM_Install*\RM\sql\oracle (e.g. C:\Program Files\Open Text\Dimensions 12.11.2 (23.4)\RM\sql\mssql).
11. Open the `create_icdba.sql` file with Notepad.
12. Select the whole file content and copy it to the clipboard (**Ctrl+C**).
13. Change back to SQL Server Management Studio.
14. Click **New Query**.
15. Paste the clipboard content into the new query window (**Ctrl+V**).
16. Replace the following values in the **DECLARE** section:
    - Replace **change_me** with the desired password for the ICDBA user account.
    - Replace **RM** with the name of your database.
17. Click **Execute**.
18. After the user account has been created, close SQL Server Management Studio.
19. Open a Windows command prompt window as administrator.
20. Navigate to *RM_Install*\RM\sql\oracle (e.g. C:\Program Files\Open Text\Dimensions 12.11.2 (23.4)\RM\bin).
21. Type the following (all on one line) and press **Enter**:
    `icManage.exe cmd_install_icdba -location` *DBNAME*
    `-icdba_password` *password*
    Replace *DBNAME* with the name of your connection specified in the System DSN, e.g. RTM.
    Replace *password* with the password you specified in point 16.

Creating the First Administrator

There are three views in RM Manage, the view is changed by clicking on one of three icons, which are, from left to right: the instance icon, the group icon, and the user icon.

RM Administrator Information

The Instance and User icons must be accessed in order to create the initial RM administrator. The administrator will, typically, be the person who creates new user accounts, creates and/or manages new instance schema and oversees the general care and feeding of RM. Complete documentation concerning user and group management can be found in the RM Administrator's Guide; as part of the installation we are including only the steps necessary to add a user account in the Administrators group.

The first account must be assigned to the already existing Administrators **group.** Please note that, even if the organization is using LDAP accounts – this RM login account should be created and used by the person(s) administering RM.

To create the Administrator Account:

a Click on the User icon (single head).

b Right click on **Users** and select **New User**.

c Enter the name of the Administrator into the box presented.

NOTE If the **Include Security Data** box was checked when the instance was created, demo users will have been created – users with names like "Joe" and "Ephoto". These names can be used for testing - or simply deleted.

d Once the user name has been entered, the details may be entered into the *New User* dialog on the right.

e From the **Group Membership** tab, highlight the **Administrators** group and click on the **Add** button to move the group to the left which will make jfogerty a member of the Administrators group.

f From the Password tab, assign a password.

g The next step is to add the user to an instance. Click on the **Instance Icon**, and from the **Group Assignment** tab, click on **Administrators** which will add the Administrators group to the RMDEMO instance. Since jfogerty is a member of the Administrators group, his name will be moved to the **Assigned** box on the left.

h From **Default Access** tab – right-click Administrators and select **Grant All** from the context menu. This setting will not actually grant all access to the administrator (this is explained in the Administrator's Guide), however it will grant all useful access.

i Open a new RM Manage (**without closing the old one**) to test login with the password settings for the administrator account.

Consideration when Importing Sample Instances

After the installation, it is helpful to create an instance from the samples provided. See the section "Configuration and the First Instance" on page 38, if you did not include an import in the post-installation tasks.

NOTE There are other options available for importing and creating instances, such as importing a blank instance to create your own world from scratch. For information about initial schema creation see the *Dimensions RM Administrator's Guide*.

The samples are provided as examples of the possibilities available with Dimensions RM. **Do NOT use** these samples as a starting point for an actual production instance. Always start with the BLANK instance or an instance of your own that was created from a BLANK instance and then saved (see the Saved Instances tab).

It is also helpful to use the sample databases for testing. If you create a script or make a schema change that causes a problem with production, you might replicate the change in a demo database and then send the details to support. This can save time for us all.

For further information about importing sample instances or backups, see chapters *"Restoring an Instance Account from a Backup"* and *"Managing Instances"* in the *Administrator's Guide*.

Importing from a Backup defined using email-rules

Considerations when creating a new instance based on an instance If you back up an instance that uses e-mail rules and then restore it to a different Dimensions RM database, the restored instance will:

- Miss out some of the rules.
- Assign some of the rules to the wrong user.

If you wish to back up and restore an instance that uses e-mail rules, please contact Micro Focus Support who will work with you to overcome these issues and successfully back up and restore the instance.

Configuring the Web Server for RM Browser

Access to Windows System TEMP Directory

If your Dimensions RM log in hangs, one possible reason may be that the user account running Tomcat does not have the requisite:

- read,
- modify, and
- delete

access to the Windows system TEMP directory. You must have such access for Dimensions RM log in to occur.

Allowing File Name Extensions for Internet Information Services (IIS)

When using Internet Information Services (IIS), you must allow certain file name extensions. If you are not using IIS, skip this chapter.

To allow file name extensions, do the following:

1. From the Windows Start menu, select `Windows Administrative Tools | Internet Information Services (IIS) Manager`.
2. Expand the server.
3. Expand **Sites**.
4. Select the desired web site, e.g. **Default Web Site**.
5. Double-click **Request Filtering**. This opens the **Request Filtering** dialog.
6. In the **Actions** pane, click **Allow File Name Extension...**. This opens the **Allow File Name Extension** dialog.
7. Enter **bmp**.
8. Click **OK**.
9. Repeat steps 6-8 for these file extensions:
   - css
   - cur
   - eot
   - exe
   - gif
   - htm
   - html
   - js
   - json
   - jsp
   - otf
   - png
   - svg
   - ttf
   - woff

- woff2
- wsdl
- xml

10 In the **Actions** pane, click **Allow File Name Extension...**. This opens the **Allow File Name Extension** dialog.

11 Type the period (.).

12 Click **OK**.

Upgrading Existing RM Instances

When upgrading from a previous RM release, the database and the instances contained within it must be upgraded to reflect the functionality and corrections delivered with the new release.

Move the `security.dat` file, stored away prior to the upgrade, into the directory specified to hold the file during installation, for example:
`C:\Program Files\Open Text\Dimensions 12.11.2 (23.4)\RM`

Wait to return the forms and javascript files until after the basic functionality has been tested.

CAUTION!

Before beginning the upgrade, make sure that you have a reliable backup of the RDBMS database installation. This requires that no users are accessing Dimensions RM while instance data is secured. To ensure this, stop these services:

Depending on upgrade status, these services may be listed under Open Text

- Micro Focus Common Tomcat
- Micro Focus Dimensions RM Pool Manager
- Micro Focus Dimensions RM E-Mail Notification Service

Note that stopping Common Tomcat will also disable other applications using this service.

Create and Restore Instances in New Database

To complete the migration, new instances must be created and populated using the .dmp files exported from original database. If the organization has special rules for naming each instance tablespace – have the DBA create a tablespace for each of the instances to be transferred – defining a tablespace consistent with the size in the *OldDB*.

1. Move all backed-up `.dmp` files onto the new Oracle server. We recommend moving them into a special "migration" folder on the Oracle Server.
2. Start RM Manage.
3. Login to the new database as the RM Administrator.
4. Right click on the database name and create the first instance on the list of instances to be restored.
5. Enter new instance information.
6. Click **OK**.
7. Click **OK** on the *Success* dialog

8 Click **EXIT** on the *Import* dialog. The instance will be listed as `pre 3.7.2` as it is essentially empty.

9 Set sizes for tablespaces (Administer Tablespaces) consistent with those used in the previous database. If this is an instance with growth potential, increase the size.

10 Right click on the newly created instance, and select **Backup/Restore Instance Account**.

11 Enter (copy and paste) the name of the folder in which the migration files are stored, and the name of the file to be restored.

12 Click on **Restore**.

13 When prompted for *From User* and *Tablespace*, enter the instance name and the name of the tablespace from the previous database (OldDB).

14 The *From user* refers to the OldDB instance name. If the organization's process was to allow RM to create the tablespace when a new instances were created – the tablespace name to be entered will also be the instance name. Check the notes created during the process "Back up Database, Instances, and Necessary Files" on page 24.

15 If a message indicating that the instance is not current is displayed, you can click on **Yes** to update.

16 Close the open dialogs, the instance should be displayed as *Current*.

17 Check group assignment and default access – if both backup and restore were performed with security, all access rights should be set as they were. Do make sure that the RM Administrator has access to the new instance.

18 Right-click on the database name and select **Change user** from the context menu. Log in as an instance administrator user.

After the first instance has been restored, check to see that all is functioning as expected from the browser before returning to Step 4 on page 90 and repeating the steps until all instances have been created and populated.

Restoring Locally Modified Files

In "Back up Database, Instances, and Necessary Files" on page 24 you were advised to back up certain files. You can now begin the restore by copying your backed up versions of Saved Projects to the new Dimensions RM 12.11.2 (23.4) installation directory.

Restoring Tomcat Files

During the setup process, a new Tomcat has been installed. This requires to carry over any local modification made to the previous Tomcat installation. To avoid overwriting, the

Common Tools folder has been renamed bearing the extension .backup, although you will also be able to reference and/or compare files from your copied folder.

IMPORTANT! This should be a merging operation, that is, the new sub-directories should be retained and only tailored/modified backup files copied to the new sub-directories. The new sub-directories in their entirety *must not* be replaced with the backup versions.

Folder Names in: RM 12.1-12.7.1	RM 12.8-12.11.2 (23.4)
RM_Install\RM\conf	*RM_Install*\RM\conf
RM_Install\Common Tools*x.x*\tomcat*x.x*\webapps\rtmBrowser\forms	*RM_Install*\Common Tools *x.x*\tomcat*x.x*\webapps\rtmBrowser\forms
RM_Install\Common Tools*x.x*\tomcat*x.x*\webapps\rtmBrowser\jscript\	*RM_Install*\Common Tools *x.x*\tomcat*x.x*\webapps\rtmBrowser\rm*\
RM_Install\Common Tools *x.x*\tomcat*x.x*\webapps\rtmBrowser\jscripts\	*RM_Install*\Common Tools*x.x*\tomcat*x.x*\webapps\rtmBrowser\rm*\

Modified forms, stored under rtmBrowser\forms in a database/class definition structure can be copied. Publish templates, stored under rtmBrowser\conf*Database_Name**Instance_Name* can also be copied.

Local changes to Tomcat configuration files (e.g., alfssogatekeeper or server.xml) can be reapplied. Taking a few minutes to do a compare in order to highlight local modifications that need to be reapplied.

Restoring Custom Headers and Footers of RM Browser Interface

This chapter applies when upgrading from Dimensions RM 12.1 or higher.

To restore your headers and footers of the RM Browser interface, follow these steps:

1. In Windows Explorer, navigate to your rtmBrowser backup directory.
   If you are installing a **regular upgrade**, this is the rtmBrowser.bak directory (refer to chapter "Restoring Tomcat Files" on page 91).
   In case you are installing a **patch**, this is the directory to which you backed up your rtmBrowser directory tree (refer to chapter "Upgrading Existing RM Instances" on page 90).
2. Open the WEB-INF folder.
3. Open the spring.xml file in a text editor.
4. Locate the last "bean id" in the file. It begins :
   `<bean id="rmHeaderAndFooterText"`
5. Beneath this entry, there are two property tags:
   - `<property name="header">`
   - `<property name="footer">`
6. Copy the above two property tags to the Clipboard.

7 In Windows Explorer, navigate to your `RM_Install\Common Tools #.#\tomcat\#.#\webapps\rtmBrowser\WEB-INF` directory.

8 Locate the last "bean id" in the file. It begins :
`<bean id="rmHeaderAndFooterText"`

9 Beneath this entry, there are two property tags:

- `<property name="header">`
- `<property name="footer">`

10 Replace the above two property tags with the Clipboard content.

11 Save the file.

Copy the files referenced in the property tags from your rtmBrowser backup to the same location of your new installation.

Example:

Your "header" property tag looks like this:

```
<property name="header"><value>/rtmBrowser/html/myheader.htm
</value></property>
```

In this case, you would copy the file `myheader.htm` from
`C:\rtmBrowser12.11.2 (23.4)_Backup\html`
to
`RM_Install\Common Tools #.#\tomcat\#.#\webapps\rtmBrowser\html.`

ALF Enabling a Dimensions RM Instance

Before a Dimensions RM instance can be used in conjunction with Application Lifecycle Framework (ALF) events, the instance must be enabled to emit ALF events and send notifications to the ALF event Manager. This is done by using the RM Manage `File | Configure ALF` options menu item. PLease see the *Administrator's Guide* for details of this menu item and how to install and configure the ALF Emitter Service.

Test Browser Access

1 Open a web browser.

2 Enter the URL to your Dimensions RM server into the URL box. The following URLs should work on the server:

- `http://localhost:`*`8080`*`/rtmBrowser/`
- `https://localhost:`*`8443`*`/rtmBrowser/`

If you modified the ports during installation, use the ports you specified.

Try also to connect from a client machine. If this fails, open the ports (8080, 8443, or the ports you specified) on the server.

IMPORTANT! For first installations, there may be no instance available and no users for web login available. If this is the case, do the following:

- Import a sample instance with the security data;
  or
- Create your own instance and user account(s).

See chapters *"Managing Instances"* and *"Managing Users and Groups"* in the *Administrator's Guide* for details.

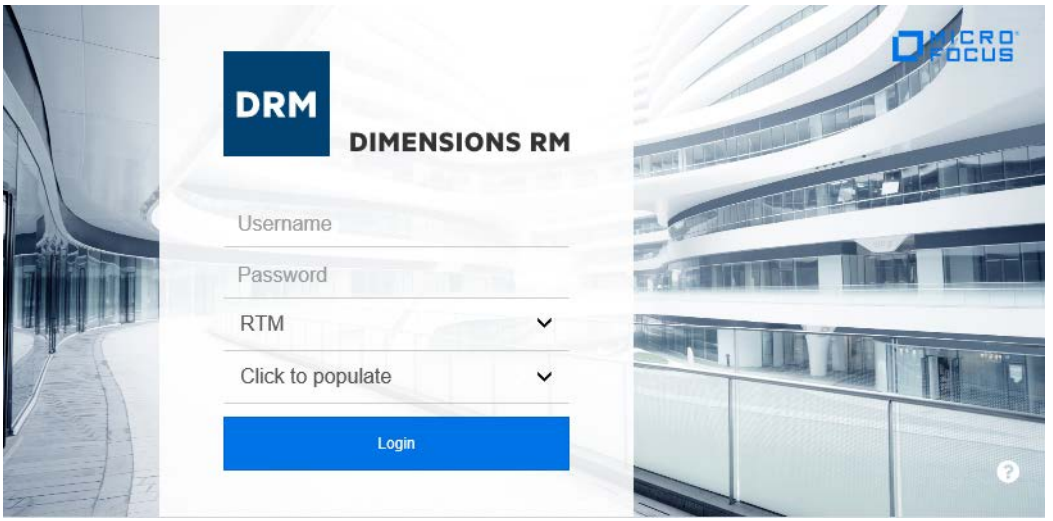


Figure 6-1. Dimensions RM Login Screen

Once you are sure that the passwords are functioning, and the browser can be accessed, step through chapter "In-Depth Check of the Dimensions RM Server" on page 94.

If there are any issues, please contact Micro Focus Support.

In-Depth Check of the Dimensions RM Server

This section describes some checks that you can perform to establish that your Dimensions RM server installation is functioning correctly:

1 For the check you require an RM instance. Please choose from the following scenarios:

- **Upgrade:** Ensure that you converted database and instance (see chapter *"Converting Database and Instances"* in the *Administrator's Guide*).
- **Fresh Install Test Environment:** Either follow the steps for the production environment, or execute these steps:

  Import the **RMDEMO** sample instance (see chapter "Consideration when Importing Sample Instances" on page 87). Ensure that you select the **Include Security Data** option as this will enable you to include user accounts, user groups, and

access right definitions in the sample instance. The chapter *"Sample Databases"* in the *Administrator's Guide* includes a list of users with their passwords for the RMDEMO sample instance.

- **Fresh Install Production Environment:**

  1. After completing the tasks in Section "Post-Installation Tasks" on page 37. you may continue with the creation of a database instance or the import of a

  2. Create a new RM instance (see chapter *"Managing Instances"* in the *Administrator's Guide*).

  3. Create a new user (see chapter *"Creating a New User"* in the *Administrator's Guide*).

  4. Assign the new user to the **Administrators** group (see chapter *"Adding a User to a Group"* in the *Administrator's Guide*).

  5. Grant all rights to the **Administrators** group (see chapter *"Setting Default User Access"* in the *Administrator's Guide*).

  6. Start the class Definition tool (see chapter *"Starting Class Definition"* in the *Administrator's Guide*).

  7. Create a generic class using the Class Definition tool (see chapter *"Adding a New Class"* in the *Administrator's Guide*) and save the class definition.

2 In RM Manage, assign a password to existing user `EPHOTO`:

a Log in to the Dimensions RM database (for example, `RM`) using:

User Name: *MyInstance*ADMIN

Password: *MyPassword*

b Click the **View User Information** toolbar button 

c In the left hand navigation tree, select user EPHOTO.

d Select the **Password** tab.

e Assign and confirm password of RTM and check **Password Never Expires**.

f Click **Accept Changes**. In some circumstances the password may already be RTM.

3 In RM Manage, define an instance schema for EPHOTO and view the class definition:

a Click the **View Instance Information** toolbar button 

b In the left hand navigation tree, right click the Dimensions RM database name, for example `RM`.

NOTE Make sure you right click on the database name (for example, `RM`) not the instance name (for example, `MYINSTANCE`).

c Select **Change User**. The **Logon Information** dialog box appears.

d Enter the following:

- User Name

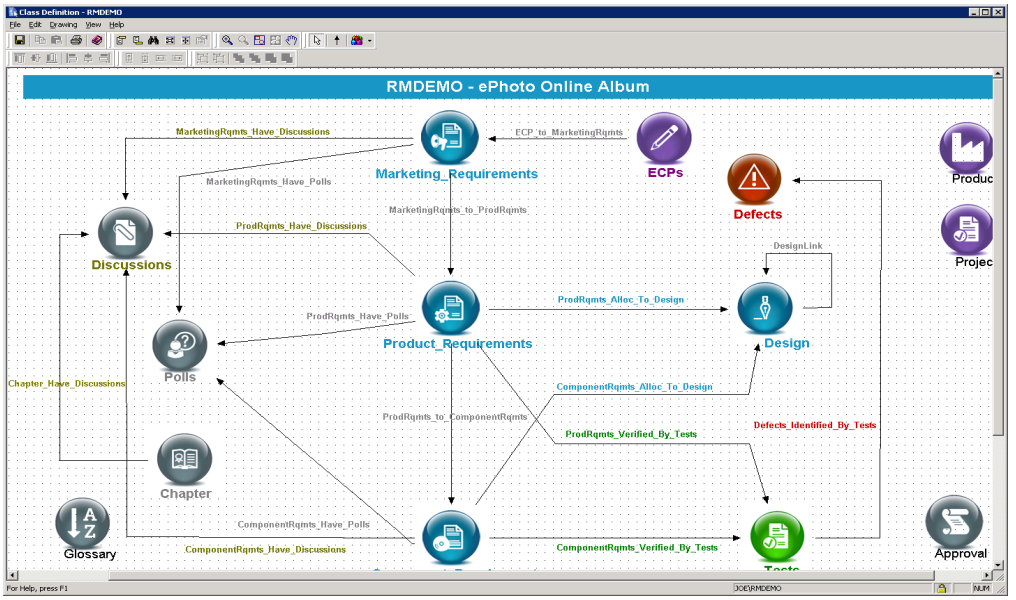
  Ephoto

- Password

  RTM

e In the left hand navigation tree, right click the Dimensions RM instance name based on the imported RMDEMO sample instance, for example MYINSTANCE.

f Select **Define Instance Schema**. After a short delay the **Class Definition** tool will open.



g Save the class definition and exit the **Class Definition** tool:

```
File | Save
File | Exit
```

h Log out of RM Manage.

4 In RM Browser, do the following:

a Log in to RM Browser.

b Export a traceability report as a Word document.

c Save the generated Word document.

d Log out of RM Browser.

5 In RM Manage, create a new group:

a Log in to the Dimensions RM database (for example, RM) using:

- User Name

  MYINSTANCEADMIN

- Password

  MYINSTANCE

b In the left hand navigation tree, single click the Dimensions RM database name, for example RM.

NOTE Make sure you single click on the database name (for example, RM) not the instance name (for example, MYINSTANCE).

c Click the **View Group Information** toolbar button

d In the left hand navigation tree, select user **Groups - <database_name>** (for example, **Groups - RM**).

e (Right click) | New Group

f Type the name of a new group, for example, `TEST`.

g Fill in a description if desired, and click **Accept Changes**.

6 In RM Manage, create a new user and assign it to the new group `TEST`:

a Click the **View User Information** toolbar button 

b In the left hand navigation tree, select user **Users - <database_name>** (for example, **Users - RM**).

c (Right click) | New User

d Type the name of a new user, for example, `TEST99`.

e Fill in a descriptions if desired, and click **Accept Changes**.

f In the left hand navigation tree, select the new user `TEST99`.

g Click the Group Membership tab.

h Select the new group `TEST` in the **Not a Member** list and click **Add** to make the new user `TEST99` a member of the new group `TEST`.

i Click the Password tab.

j Assign a permanent password to the new user `TEST99`, for example, `TEST99`.

7 In RM Manage, assign the new group `TEST` and new user `TEST99` to the `MYINSTANCE` instance and grant all access:

a Click the **View Instance Information** toolbar button  or `View | Instances`.

b In the left hand navigation tree, right click the Dimensions RM instance name based on the imported `RMDEMO` sample instance, for example `MYINSTANCE`.

c Click the Group Assignment tab.

d In the **Assign groups/users to instance MYINSTANCE** region, check the new group `TEST`.

e Click the Default Access tab.

f Right click on the new group `TEST` and select **Grant All**.

g Right click on the new user `TEST99` and select **Grant All**.

h Log out of RM Manage.

8 In RM Browser, export a traceability report for the new user TEST99:

a Log in to RM Browser with user TEST99.

b Export a traceability report as a Word document.

c Save the generated Word document.

9 In RM Browser, create a requirement for the logged in user TEST99 and log out of RM Browser.

The Dimensions RM server quick installation checks are now complete. If there are any problems, please contact Micro Focus Support.

Appendix A

SSO, SSL and Certificates

SSO and CAC Configuration

The Micro Focus Single Sign On (SSO) option in the Dimensions RM installer installs components needed for the RM server to communicate with a Micro Focus SSO server. For detailed information concerning the installation and configuration of the Micro Focus SSO server, see the Dimensions CM or SBM documentation.

Exporting a Certificate from the STS Server

After you have configured the Dimensions CM or SBM STS server, you must export a certificate from the STS server and then copy it to the RM Server.

To export the STS certificate from the STS server, do the following:

1 Execute the steps described in chapter "Exporting a Certificate from the STS Server from the Command Prompt" on page 116 or "Exporting the STS Certificate from SBM Configurator" on page 117.

IMPORTANT! Ensure that you retrieve the certificate in **PEM** format.

2 Copy the resulting ***sts.pem*** file to ***RM_Install***\RM\conf (e.g. *C:\Program Files\Micro Focus\Dimensions 12.11.2 (23.4)*\RM\conf). Verify that the value of the registry key SSO_TRUST_CERTIFICATE matches the actual location of the file. See "RM Server Parameters" on page 103.

Adding a Certificate for RM Server to the STS Keystore

The RM server certificate has to be added to a configured truststore (the default file name is truststore.jks).

To add the RM Server certificate to the STS keystore, do the following:

1 Execute the steps described in chapter "Exporting Certificates to CER Format from the Management Console" on page 111 or "Exporting Certificates to CER Format from IIS" on page 112.

2 Open a command prompt.

3 Type keytool and press **Enter**. If you receive the message that keytool is not recognized, type the following command and press **Enter**:
set path=%path%;"***RM_Install***\Common Tools ***#.#.#.#***\jre***#.#***\bin"

NOTE

- Replace ***RM_Install*** with the path to the Dimensions RM directory, e.g. *C:\Program Files\Micro Focus\Dimensions 12.11.2 (23.4)*.
- Replace **#.#.#.#** with the Common Tools version number, e.g. *1.8.6.0*.
- Replace **#.#** with the Java version number, e.g. 11.0.

The complete set command may look like this:

set path=%path%;"*C:\Program Files\Micro Focus\Dimensions* 12.11.2 (23.4)\Common Tools *1.8.6.0*\jre*11.0*\bin"

4 Navigate to the location of the truststore, which is at *SBM_Install*\Common\Tomcat #.#\server\default\webapps\idp\WEB-INF\conf.

NOTE Starting with SBM version 2009R4.01, truststore.jks contains a demo Dimensions RM server certificate. If you import your own certificate with the suggested alias **rmserver**, type the following command and press **Enter**:

```
keytool -delete -alias rmserver
-keystore truststore.jks -storepass StorePassword
```

- Replace *StorePassword* with the password for the keystore.
  The default password for the truststore.jks keystore is: **changeit**

5 Type the following command (all on one line) and press **Enter**:

```
keytool -import -trustcacerts
-keystore TruststoreName -storepass StorePassword
-alias Alias -file CerPath
```

NOTE

- Replace *TruststoreName* with the file name of the truststore. The default is truststore.jks. If the keystore name contains spaces, surround it with double quotes.
- Replace *StorePassword* with the password for the keystore.
  The default password for the cacerts keystore is: **changeit**
- Replace *Alias* with a unique name.
  Suggested aliases:
  - rm_ca for a CA certificate.
  - rmserver for the RM server certificate.
- Replace *CerPath* with the full path to your certificate in CER format. If the path contains spaces, surround the path with double quotes.

The complete keytool command may look like this (all on one line):

```
keytool -import -trustcacerts -keystore truststore.jks
-alias rmserver -file "C:\My Certificates\MyCert.cer"
```

Enabling SSO as a Login Source

Before you can use SSO authentication with RM instances, you must enable SSO as a login source for the database that contains those instances. It is possible, with Dimensions RM to assign multiple login sources, and to order their selection.

Please see the Section *Configuring Login Sources,* in the RM *Dimensions RM Administrator's Guide* for full details.

Configuring SSL Certificates

You must create and configure SSL certificates to ensure security. See the Dimensions CM or SBM documentation for general information on the creation and configuration of SSL certificates for Micro Focus SSO.

NOTE For initial setup and testing, demonstration certificates are included in the installation. These are not intended for production use and should be replaced with your own certificates. See the Dimensions CM or SBM documentation.

- Create a certificate for the RM server (RM_CERT). Configure the STS server to trust this certificate. The certificate can be either self-signed or signed by a certificate authority (CA_RM_CERT).

NOTE To communicate with the Micro Focus SSO server (STS server), your RM Server and fat client systems must include a copy of the STS server certificate.

- Please see the following:
  - "Exporting a Certificate from IIS" on page 102,
  - "Exporting a Certificate from the STS Server" on page 100
  - "Adding a Certificate for RM Server to the STS Keystore" on page 100.
- Create a certificate for the RM web server (RM_WEB_CERT). To enable SSO with remote fat clients, the RM web server should be configured for SSL and the certificate should be signed by a known certificate authority.

IMPORTANT! Remote fat clients use SSL when connecting to RM Server to avoid transferring plain-text passwords and certificates over the network.

Exporting a Certificate from IIS

When you have configured the RM Web Server to use an SSL certificate (which you should do before production use), then you must configure the Admin clients to use the same CA certificate as was used to sign the certificate for the RM Web Server. The CA certificate must be in PEM format.

NOTE The following example procedure shows how to export a CA certificate from IIS server. However, as Dimensions RM includes its own Tomcat web server, Apache and IIS are not required. Given the server implementation and corporate security measures you may run a third-party web server in addition to the Open Text Common Tomcat web server.

1. Retrieve the certificate in CER format by following the steps in chapter "Exporting Certificates to CER Format from IIS" on page 112.

2 Use the openssl tool to convert the file to PEM format as in this example:
```
openssl x509 -in exported_certificate.cer -out
certificate_for_rm.pem -inform DER -outform PEM
```

NOTE

- Do not use a self-signed certificate on the RM Web Server.
- You can obtain an openssl binary from http://www.openssl.org/

Verifying Registry Keys and Configuration Files on the RM Server

The following lists the registry keys and configuration files located on the RM server system that are necessary to implement SSO. This may be of use in troubleshooting the configuration.

RM Server Parameters

```
HKEY_LOCAL_MACHINE\SOFTWARE\Micro Focus\Dimensions RM\Environment\Defau
lt
```

RM Server Registry Keys	
Key	**Description**
RMKey (String)	Contains a full path to a file with a private key of the RM server certificate. The Key file should not be password protected. The file must be in .pem format. Example: `C:\Program Files\Micro Focus\Dimensions 12.11 .2 (23.4)\RM\conf\rmkey.pem`
RMCertificate (String)	Contains a full path to a file for a certificate of the RM server. The file must be in .pem format. Example: `C:\Program Files\Micro Focus\Dimensions 12.11 .2 (23.4)\RM\conf\rmcert.pem`
SSOServer (String)	Contains the URL to the SSO/STS server. Only the host name and port are required. Example: `http://ssohost:8085`
STSServer (String)	Contains the URL to the STS server if it is installed separately. This is optional and is not needed when SSO is provided by SBM only.
SSO_TRUST_CERTIFICATE	Contains the full path to the STS server certificate. Example: `C:\Program Files\Micro Focus\Dimensions 12.11 .2 (23.4)\RM\conf\sts.pem`

RM Server Registry Keys	
Key	**Description**
SSO_RELYING_PARTY	Should contain the SSO "Relaying Party" used to validate and request Token. For more information about this value, read the STS server configuration information Contains a default value of: `uri:org:eclipse:alf:sso:relyingparty :anonymous:anonymous:anonymous;uri :org:eclipse:alf:sso:relyingparty :serena.application.engine .notification.server:anonymous :anonymous`
SSO_CLOCK_TOLERANCE	"Expiration Tolerance" time in sec, used to validate the STS Token. Sometimes clocks (server and relying party) are not perfectly aligned. A token might be issued say at 12:00:00 but the Relying Party might be 2-3 minutes behind so it is 11:57:00. In such a case, the token will be needlessly rejected. So we need to have a small (configurable) amount of time that allows for clock skew. Value set by the installer: `300`

Gatekeeper Parameters

The Gatekeeper runs on the Open Text Common Tomcat web server. Its parameters are contained in two configuration files located in the following directory (the beginning of the path varies depending on which Open Text product the Tomcat installation is from):

Installation_Path\Common Tools *X.X.X*\tomcat*X.X*\alfssogatekeeper\conf

IMPORTANT! Ensure that the gatekeeper configuration specifies the same host names in Dimensions RM as in SBM or Dimensions CM. Specify host names rather than IP addresses, otherwise SSO may not work correctly with Web applications.

gatekeeper-core-config.xml	
Parameter	**Description**
SecurityTokenService	URL to the STS server. This is configured by the installer. Example: `http://sts-server:8085/TokenService/ services/Trust`
SecurityTokenServiceExternal	Same as the SecurityTokenService.
FederationServerURL	URL to the Federation server. This is configured by the installer. Example: `http://sts-server:8085/ALFSSOLogin/login`

gatekeeper-services-config.xml	
Parameter	**Description**
Path: <GatekeeperProtectionControl> <ProtectedURIs> Element: <URIMatcher requestURI="/rtmBrowser/*" />	URIMatcher should have one line that contains "/rtmBrowser/*" string. This is a definition of a filter to protect a particular web application.
Path: <Service name="default" ProtectionLevel="all"> <ServiceEntryPoints> <BrowserRequests> Element: <URIMatcher requestURI="/rtmBrowser/*" />	Protected URL mask.
Path: <GlobalLogoutURI> Element: <URIMatcher requestURI="/*/logout-sso.jsp" />	The default logout URL to use with the sequence to invalidate SSO token. When accessing this URL, the Gatekeeper automatically rejects the SSO token causing the login screen to appear.
Path: <DMZ> <BrowserRequests> Elements: <URIMatcher requestURI="/rtmBrowser/css/*"/> <URIMatcher requestURI="/rtmBrowser/html/*"/> <URIMatcher requestURI="/rtmBrowser/images/*"/> <URIMatcher requestURI="/rtmBrowser/imagesnew/*"/> <URIMatcher requestURI="/rtmBrowser/jscript/*"/> <URIMatcher requestURI="/rtmBrowser/jscripts/*"/> <URIMatcher requestURI="/rtmBrowser/WebServices"/> <URIMatcher requestURI="/rtmBrowser/WebServices/rtmService.wsdl"/> <URIMatcher requestURI="/rtmBrowser/Command"/>	

Verifying Registry Keys and Configuration Files on the Fat Client

The following lists the SSO-related registry keys and configuration files located on systems with a fat client installation. This may be of use in troubleshooting the configuration.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Micro Focus\Dimensions RM\Environment\Defau
lt
```

RM Fat Client Registry Keys	
Key	**Description**
RMKey (String) (Optional)	Contains a full path to a file with a private key of the RM server certificate. The Key file should not be password protected. The file must be in .pem format. Example: `C:\Program Files\Micro Focus\Dimensions 12.11.2 (23.4)\RM\conf\rmkey.pem`
RMCertificate (String) (Optional)	Contains a full path to a file for a certificate of the RM server. The file must be in .pem format. Example: `C:\Program Files\Micro Focus\Dimensions 12.11.2 (23.4)\RM\conf\rmcert.pem`
SSOServer (String)	Contains the URL to the Dimensions CM or SBM SSO/STS server. Only the host name and port are required. Example: `http://ssohost:8085`

RMServer
(String)
	Contains the URL to the RM server.
	
	Fat clients communicate with the RM server to request an SSO token. This registry key allows the use of non-standard ports. Remote fat clients must use HTTPS, so the URL must contain https for the protocol portion of the URL.
	
	To use a specific port:
	`https://rmserverhost:8443`
	To use a the default HTTPS port:
	`https://rmserverhost3`

CAC (String) (Optional)	If this key contains a non-empty value, CAC logins are "enforced". In such a case, a user can be validated as a "pure" RM local user or by using smart cards. If this key doesn't exist, a user can be validated with SSO using a username/password combination.
CACertificate (String)	Contains the full path to a file with the CA_RM_WEB (a trusted issuer of the certificate) to validate the RM web server certificate. The file must be in .pem format. **NOTE** Connection to RM Web uses SSL only, therefore this setting is important.

Troubleshooting SSO, SSL

1. **Please review the section Verifying Registry Keys and Configuration Files on the RM Server103.** This lists the registry keys and configuration files located on the RM server system and necessary to implement SSO.
2. **Certificate sts.pem mismatch**
   Update the certificate as described in chapter Table , "Exporting a Certificate from the STS Server," on page 100.
3. **LDAP Server unavailable**
   If you are using LDAP with SSO, check that the LDAP server is available. With SBM, you perform this check with the SBM Configurator.

Redirecting Internal Web Service and REST Service Calls

When using a setup where an Apache server or Microsoft IIS is used in combination with Tomcat, HTTPS calls may not work or show poor performance. This can be resolved by redirecting those calls so that the Apache server or Microsoft IIS is not used.

To redirect internal web service calls, do the following:

1. Open Windows Registry editor (select **Run**, enter `regedit` and click **OK**).
2. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Micro Focus\Dimensions RM\Environment\Default`.
3. Right-click the **Default** key and select **`New | String Value`** from the shortcut menu.
4. Specify the name `RM_INTERNAL_WS_URL` and press **Enter**.
5. Double-click the `RM_INTERNAL_WS_URL` value. This opens the **Edit String** dialog.
6. Enter the server URL into the **Value data** box, e.g. *`http://localhost:8080/`*

   If HTTP is not enabled, change the URL protocol to https.

   Change the port to match your Tomcat configuration.
7. Click **OK**.

To redirect internal REST service calls, do the following:

1. Open Windows Registry editor (select **Run**, enter `regedit` and click **OK**).
2. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Micro Focus\Dimensions RM\Environment\Default`.
3. Right-click the **Default** key and select **`New | String Value`** from the shortcut menu.
4. Specify the name `RM_INTERNAL_REST_URL` and press **Enter**.

5 Double-click the RM_INTERNAL_REST_URL value. This opens the **Edit String** dialog.

6 Enter the server URL into the **Value data** box, e.g. *http://localhost:8080/*

If HTTP is not enabled, change the URL protocol to https.

Change the port to match your Tomcat configuration.

7 Click **OK**.

Importing a PFX Certificate into Microsoft IIS

If you are using Solutions Business Manager (SBM), use SBM Configurator to import the certificate into IIS, as this also configures SBM to use the certificate. In this case, you do not have to execute the following steps.

To import a PFX certificate into IIS, do the following:

1. On the server, start **Server Manager**.
2. Expand **Roles**.
3. Expand **Web Server (IIS)**.
4. Select **Internet Information Services (IIS) Manager**.
5. In **Internet Information Services (IIS) Manager**, select your server.
6. On the servers **Home** view, double-click **Server Certificates**.
7. In the **Actions** pane, click **Import...**
8. Click **...**. This opens the **Open** dialog.
9. Select the PFX certificate and click **Open**.
10. Enter the password into the **Password** box.
11. Ensure that the option **Allow this certificate to be exported** is selected.
12. Click **OK**.

Importing a PFX Certificate into Windows

If you are using IIS, you only need to execute the steps described in chapter "SSO and CAC Configuration" on page 100. You only need to execute the following steps if you are not using IIS.

To import a certificate to PFX format, do the following:

1. On the server, open a command prompt.
2. Enter `mmc` and press **Enter** to start the Microsoft Management Console.
3. From the **File** menu, select **Add/Remove Snap-in...** or press **Ctrl+M**.
4. From the list **Available snap-ins**, select **Certificates**.
5. Click **Add**.
6. In the **Certificates snap-in** dialog, do the following:
   a. Select **Computer account**.
   b. Click **Next**.
   c. Ensure that option **Local computer: (the computer this console is running on)** is selected.

d Click **Finish**.

7 Click **OK**.

8 Expand **Certificates (Local Computer)**.

9 Expand **Personal**.

10 Select **Certificates**, if it exists. This lists all personal certificates and allows you to check if the certificate has been imported before.

11 Right-click **Personal**. This opens a shortcut menu.

12 Point to **All Tasks**, then select **Import...**. This opens the **Certificate Import Wizard**.

13 Click **Next**.

14 Click **Browse...**. This opens the **Open** dialog.

15 In the file filter box, select **Personal Information Exchange (*.pfx;*.p12)**.

16 Select the PFX certificate and click **Open**.

17 Click **Next**.

18 Enter the password into the **Password** box.

19 Select the option **Make this key exportable. This will allow you to back up or transport your keys at a later time**.

20 Ensure that the option **Allow this certificate to be exported** is selected.

21 Click **Next**.

22 Ensure the following:

a The option **Place all certificates in the following store** is selected.

b The **Certificate store** box shows **Personal**.

If this is not the case, do the following:

c Select the option **Place all certificates in the following store**.

d Click **Browse...**. This opens the **Select Certificate Store** dialog.

e Select **Personal** and click **OK**.

23 Click **Next**.

24 Click **Finish** and confirm the success message.

Exporting Certificates

Exporting Certificates to CER Format from the Management Console

The CER format is used for import into most keystores. For the SSL keystore (e.g. sample-ssl.jks) in Tomcat's conf directory, a PFX certificate is required (see chapter "Exporting Certificates to PFX Format from the Management Console" on page 113).

The following steps assume that the certificate is available on the web server, and imported to Windows.

To export a certificate to CER format, execute these steps:

1. On the server, open a command prompt.
2. Enter `mmc` and press **Enter** to start the Microsoft Management Console.
3. From the **File** menu, select **Add/Remove Snap-in...** or press **Ctrl+M**.
4. From the list **Available snap-ins**, select **Certificates**.
5. Click **Add**.
6. In the **Certificates snap-in** dialog, do the following:
   a. Select **Computer account**.
   b. Click **Next**.
   c. Ensure that option **Local computer: (the computer this console is running on)** is selected.
   d. Click **Finish**.
7. Click **OK**.
8. Expand **Certificates (Local Computer)**.
9. Locate the certificate in the tree. Common locations are:
   - `Personal | Certificates`
   - `Trusted Root Certification Authorities | Certificates`
10. Right-click the certificate and select `All Tasks | Export` from the shortcut menu. This opens the **Certificate Export Wizard**.
11. Click **Next**.
12. Ensure that option **No, do not export the private key** is selected.
13. Click **Next**.
14. Ensure that option **DER encoded binary X.509 (.CER)** is selected.
15. Click **Next**.
16. Click **Browse...** to open a dialog to save the certificate.
17. Select the target directory and specify a file name.

18 Click **Save**.

19 Click **Next**.

20 Click **Finish** and confirm the success message.

21 Double-click the certificate and select the **Certification Path** tab.

22 If there are other certificates referenced, do the following:

- **a** Select the certificate.
- **b** Click **View Certificate**.
- **c** Select the **Details** tab.
- **d** Click **Copy to File...**. This opens the **Certificate Export Wizard** for the selected certificate.
- **e** Ensure that the option **DER encoded binary X.509 (.CER)** is selected.
- **f** Click **Next**.
- **g** Click **Browse...** to open a dialog to save the certificate.
- **h** Select the target directory and specify a file name.
- **i** Click **Save**.
- **j** Click **Next**.
- **k** Click **Finish** and confirm the success message.
- **l** Click **OK** to close the certificate.
- **m** Repeat steps a-l for any other certificate in the certification path (except for your server, which you exported already with steps 10-20).

Exporting Certificates to CER Format from IIS

The CER format is used for import into most keystores. For the SSL keystore (e.g. sample-ssl.jks) in Tomcat's conf directory, a PFX certificate is required (see chapter "Exporting Certificates to PFX Format from the Management Console" on page 113).

The following steps assume that the certificate is available on the Internet Information Server (IIS).

To export a certificate to CER format, execute these steps:

1 Start the **Computer Management Console** by running the command `compmgmt.msc`. Alternatively you can right-click on the Computer icon and select **Manage** from the resulting menu.

2 Locate **Internet Information Server (IIS) Manager**.

3 Select a computer node.

4 From the **Home** list, locate the **Server Certificates** icon and expand it.

5 Locate the IIS certificate from the list and open it.

6 From the opened dialog, switch to the **Certification Path** tab.

7 Select a CA certificate from the list and open it.

8 From the opened dialog, switch to the **Details** tab.

9 Click **Copy to File**. This opens the **Certificate Export Wizard**.

10 Click **Next**.

11 Ensure that option **No, do not export the private key** is selected.

12 Click **Next**.

13 Ensure that option **DER encoded binary X.509 (.CER)** is selected.

14 Click **Next**.

15 Click **Browse...** to open a dialog to save the certificate.

16 Select the target directory and specify a file name.

17 Click **Save**.

18 Click **Next**.

19 Click **Finish** and confirm the success message.

20 Use an openssl tool to convert the file to `.PEM` format as in this example:
`openssl x509 -in exported_certificate.cer -out certificate_for_rm.pem -inform DER -outform PEM`

NOTE

- Do not use a self-signed certificate on the RM Web Server.
- You can obtain an openssl binary from http://www.openssl.org/

Exporting Certificates to PFX Format from the Management Console

A certificate in PFX format is required for import into the ssl keystore (e.g. sample-ssl.jks) in Tomcat's `conf` directory. For all other keystores, use the CER format (see chapter "Exporting Certificates to CER Format from the Management Console" on page 111).

The following steps assume that the certificate is available on the web server, and imported to Windows.

To export a certificate to PFX format, execute these steps:

1 On the server, open a command prompt.

2 Enter `mmc` and press **Enter** to start the Microsoft Management Console.

3 From the **File** menu, select **Add/Remove Snap-in...** or press **Ctrl+M**.

4 From the list **Available snap-ins**, select **Certificates**.

5 Click **Add**.

6 In the **Certificates snap-in** dialog, do the following:

   a Select **Computer account**.

   b Click **Next**.

   c Ensure that option **Local computer: (the computer this console is running on)** is selected.

   d Click **Finish**.

7 Click **OK**.

8 Expand **Certificates (Local Computer)**.

9 Locate the certificate in the tree. Common locations are:

   - `Personal | Certificates`
   - `Trusted Root Certification Authorities | Certificates`

10 Right-click the certificate and select `All Tasks | Export` from the shortcut menu. This opens the **Certificate Export Wizard**.

11 Click **Next**.

12 Select the option **Yes, export the private key**.

13 Click **Next**.

14 Ensure that option **Personal Information Exchange - PKCS #12 (.PFX)** is selected.

15 Select the following options:

   - **Include all certificates in the certification path if possible**
   - **Export all extended properties**

16 Click **Next**.

17 Enter a password into the **Password** and **Type and confirm password (mandatory)** boxes. Take a note of that password.

18 Click **Next**.

19 Click **Browse...** to open a dialog to save the certificate.

20 Select the target directory and specify a file name.

21 Click **Save**.

22 Click **Next**.

23 Click **Finish** and confirm the success message.

Exporting Certificates to PFX Format from IIS

A certificate in PFX format is required for import into the ssl keystore (e.g. sample-ssl.jks) in Tomcat's `conf` directory. For all other keystores, use the CER format (see chapter "Exporting Certificates to CER Format from the Management Console" on page 111).

The following steps assume that the certificate is available on the Internet Information Server (IIS).

To export a certificate to PFX format, execute these steps:

1. Do one of the following:
   - Start the **Server Manager**, and expand **Roles** followed by **Web Server (IIS)**.
   - Start the **Computer Management Console** by running the command `compmgmt.msc`, and expand **Services and Applications**.
   - Right-click on the Computer icon, select **Manage** from the resulting menu, and expand **Services and Applications**.
2. Select **Internet Information Server (IIS) Manager**.
3. In the **Connections** pane, select a computer node.
4. On the **Home** pane, double-click the **Server Certificates** icon.
5. Double-click the IIS certificate. This opens the **Certificate** dialog.
6. Select the **Details** tab.
7. Click **Copy to File**. This opens the **Certificate Export Wizard**.
8. Click **Next**.
9. Select the option **Yes, export the private key**.
10. Click **Next**.
11. Ensure that option **Personal Information Exchange - PKCS #12 (.PFX)** is selected.
12. Select the following options:
    - **Include all certificates in the certification path if possible**
    - **Export all extended properties**
13. Click **Next**.
14. Enter a password into the **Password** and **Type and confirm password (mandatory)** boxes. Take a note of that password.
15. Click **Next**.
16. Click **Browse...** to open a dialog to save the certificate.
17. Select the target directory and specify a file name.
18. Click **Save**.
19. Click **Next**.
20. Click **Finish** and confirm the success message.

NOTE Do not use a self-signed certificate on the RM Web Server.

Exporting a Certificate from the STS Server from the Command Prompt

When using SBM, you can export the STS certificate through SBM configurator (see chapter "Exporting the STS Certificate from SBM Configurator" on page 117).

To export the STS certificate, do the following:

1. From a command prompt, navigate to the following directory on the STS server:
   `TokenService.war\WEB-INF\conf`
2. Type `keytool` and press **Enter**. If you receive the message that keytool is not recognized, type the following command and press **Enter**:
   `set path=%path%;"RM_Install\Common Tools #.#.#.#\jre\#.#\bin"`

NOTE

- Replace *RM_Install* with the path to the Dimensions RM directory, e.g. *C:\Program Files\Micro Focus\Dimensions 12.11.2 (23.4)*.
- Replace **#.#.#.#** with the Common Tools version number, e.g. *1.8.6.0*.
- Replace **#.#** with the Java version number, e.g. 11.0.

The complete set command may look like this:

```
set path=%path%;"C:\Program Files\Micro Focus\Dimensions 12.11.2
(23.4)\Common Tools 1.8.6.0\jre\11.0\bin"
```

3. Type the following command (all on one line) and press **Enter**:
   ```
   keytool -export
   -keystore keystore.jks -storepass StorePassword
   -alias sts -file CerPath
   ```

NOTE

- Replace *StorePassword* with the password for the keystore. The default for keystore.jks is **changeit**
- Replace *CerPath* with the full path to your certificate in CER format. If the path contains spaces, surround the path with double quotes.

The complete keytool command may look like this (all on one line):

```
keytool -export -keystore keystore.jks -storepass MyPassword
-alias sts -file "C:\My Certificates\MyCert.cer"
```

4 To convert the certificate to PEM format, type the following openssl command and press **Enter**:
`openssl x509 -in CerPath -inform DER -out PemPath -outform PEM`

NOTE

- You can obtain an openssl binary from http://www.openssl.org/.
- Replace *CerPath* with the full path to your certificate in CER format. If the path contains spaces, surround the path with double quotes.
- Replace *PemPath* with the full path you want to save the certificate in PEM format to. If the path contains spaces, surround the path with double quotes.

The complete keytool command may look like this (all on one line):

```
openssl x509 -in "C:\My Certificates\MyCert.cer" -inform DER
-out "C:\My Certificates\MyCert.pem" -outform PEM
```

Exporting the STS Certificate from SBM Configurator

When using SBM, you can export the STS certificate through SBM configurator, which allows exporting the certificate into various formats.

To export the STS certificate, do the following:

1 Start **SBM Configurator**.

2 In the **Advanced** set, select **Security**.

3 In the **Components** list, ensure that **STS** is selected.

4 Click **Actions**. This opens a shortcut menu.

5 From the shortcut menu, select **Export Certificate**. This opens the **Save As** dialog.

6 In the **Save as type** box, select the desired format.

NOTE

- If you require the certificate for copying it to *RM_Install*`\RM\conf`, choose **(*.pem)**.
- If you require the certificate for importing it into a keystore (e.g. truststore.jks), choose **(*.cer)**.

7 Navigate to a directory to which you want to save the file to.

8 Enter a file name (e.g. `sts.pem` or **sts.cer** depending on the Save as type setting) into the **File name** box.

9 Click **Save** and confirm the success message.

Listing all Certificates in a Keystore

To retrieve the alias, execute these steps:

1 Open a command prompt and navigate to the directory where the keystore is located.

2 Type `keytool` and press **Enter**. If you receive the message that keytool is not recognized, type the following command and press **Enter**:
`set path=%path%;"RM_Install\Common Tools #.#.#.#\jre\#.#\bin"`

NOTE

- Replace *RM_Install* with the path to the Dimensions RM directory, e.g. *C:\Program Files\Micro Focus\Dimensions 12.11.2 (23.4)*.
- Replace **#.#.#.#** with the Common Tools version number, e.g. *1.8.6.0*.
- Replace **#.#** with the Java version number, e.g. 11.0.

The complete set command may look like this:

`set path=%path%;"C:\Program Files\Micro Focus\Dimensions 12.11.2 (23.4)\Common Tools 1.8.6.0\jre\11.0\bin"`

3 Type the following command (all on one line) and press **Enter**:
`keytool -list -v -keystore Keystore -storepass StorePassword >certs.txt`

NOTE

- Replace *Keystore* with the path to the desired keystore. If the path contains spaces, surround the path with double quotes.
- Replace *StorePassword* with the password for the keystore.

The complete keytool command may look like this (all on one line):

`keytool -list -v -keystore sample-ssl.jks -storepass serena >certs.txt`

4 Type `notepad certs.txt` and press **Enter**. This opens the file certs.txt in Notepad. The file certs.txt contains detailed information about all certificates in the keystore.

Retrieving the Alias from a PFX File

When importing the certificate into the Micro Focus Common Tomcat, the alias used in the PFX file is required.

To retrieve the alias, execute these steps:

1 Open a command prompt and navigate to the directory where the PFX file is located.

2 Type `keytool` and press **Enter**. If you receive the message that keytool is not recognized, type the following command and press **Enter**:
`set path=%path%;"`***`RM_Install`***`\Common Tools `***`#.#.#.#`***`\jre\`***`#.#`***`\bin"`

NOTE

- Replace ***RM_Install*** with the path to the Dimensions RM directory, e.g. *C:\Program Files\Micro Focus\Dimensions 12.11.2 (23.4)*.
- Replace **#.#.#.#** with the Common Tools version number, e.g. *1.8.6.0*.
- Replace **#.#** with the Java version number, e.g. 11.0.

The complete set command may look like this:

`set path=%path%;"`*`C:\Program Files\Micro Focus\Dimensions`* `12.11.2 (23.4)\Common Tools `*`1.8.6.0`*`\jre\`*`11.0`*`\bin"`

3 Type the following command (all on one line) and press **Enter**:
`keytool -list -v`
`-keystore `***`PfxCertificate`*** `-storepass `***`PfxPassword`*** `>pfx.txt`

NOTE

- Replace ***PfxCertificate*** with the file name of your PFX certificate. If the file name contains spaces, surround the file name with double quotes.
- Replace ***PfxPassword*** with the password for the PFX certificate. If you exported the certificate as described in chapter "Exporting Certificates to PFX Format from the Management Console," use the password you specified on export.

The complete keytool command may look like this (all on one line):

`keytool -list -v`
`-keystore `***`MyCertificate.pfx`*** `-storepass `***`topsecret`*** `>certs.txt`

4 Type `notepad pfx.txt` and press **Enter**. This opens the file pfx.txt in Notepad.

5 Locate the line starting with **Alias name** and write down the value. In this example, the alias name is 1: **`Alias name:`** *1*

Retrieving Root CA and Intermediate CA Certificate Files from a Certificate

A certificate usually contains several Certification Authority certificates, which confirm the validity. If you require the certificates of these certificates as separate files, you need to extract them from the certificate. The following steps show how to that for both, PFX and CER certificates.

A certificate path may look like this:

- Root CA
  - Intermediate CA
    - Server

There may be several intermediate CAs in a certificate. If you require the intermediate CA files, you need to export all of them.

Retrieving Root CA and Intermediate CA Certificate Files from a PFX File

As PFX files cannot be opened directly, you need to open it in the Certificate Manager.

To open a PFX certificate in the Certificate Manager, execute these steps:

1. Open a command prompt.
2. Type `certmgr` and press **Enter**. This starts the Certificate Manager.
3. Locate the certificate in the tree. A common location may be `Personal | Certificates`.

   If you cannot find the certificate, you need to (temporarily) import it by executing these steps:

   a. Right-click the **Personal** folder. In the shortcut menu, point to **All Tasks**, and then select **Import...**. This opens the **Certificate Import Wizard**.

   b. Click **Next**.

   c. Click **Browse...**.

   d. From the file filter box, select **Personal Information Exchange (*.pfx;*.p12)**.

   e. Select the PFX file and click **Open**.

   f. Click **Next**.

   g. In the **Password** box, type the current password for the PFX file.

   h. Click **Next**.

   i. Click **Next**.

   j. Click **Finish** to import the file and confirm the success message.

   k. In the tree, expand **Personal**, then select **Certificates**.
4. Double-click the Certificate. This opens the **Certificate** dialog. Continue with step 2 in chapter "Retrieving Root CA and Intermediate CA Certificate Files from a CER File" on page 120.

Retrieving Root CA and Intermediate CA Certificate Files from a CER File

The following steps describe how to retrieve root CA and intermediate CA certificates from a server certificate file in CER format. Depending on your certificate, there may be no root CA and/or intermediate CA certificates.

To retrieve root CA and intermediate CA certificate files from a CER file, do the following:

1. Double-click the CER file. This opens the **Certificate** dialog.

2 Select the **Certification Path** tab.

3 If you see only one entry (your server name), there are no root CA and intermediate CAs. Skip all further steps.

4 Select the top certificate (this is the root CA).

5 Click **View Certificate**. This opens the selected certificate.

6 Select the **Details** tab.

7 Click **Copy to File...**. This opens the **Certificate Export Wizard**.

8 Click **Next**.

9 Select the export format, e.g. **DER-encoded binary X.509 (.CER)**.

10 Click **Next**.

11 Click **Browse...** to specify the path/file name to which you want to export the certificate.

12 Click **Next**.

13 Click **Finish** and confirm the success message.

14 Click **OK** to close the certificate.

15 If there are certificates between the root CA certificate and the server certificate, select each of them and execute steps 5-14.

Importing Root CA and Intermediate CA certificates into the Local Machine Certificate Store

To import a root CA certificate and/or an intermediate CA certificate in CER format, do the following:

1 On the server, open a command prompt.

2 Enter `mmc` and press **Enter** to start the Microsoft Management Console.

3 From the **File** menu, select **Add/Remove Snap-in...** or press **Ctrl+M**.

4 From the list **Available snap-ins**, select **Certificates**.

5 Click **Add**.

6 In the **Certificates snap-in** dialog, do the following:

   a Select **Computer account**.

   b Click **Next**.

   c Ensure that option **Local computer: (the computer this console is running on)** is selected.

   d Click **Finish**.

7 Click **OK**.

8 Expand **Certificates (Local Computer)**.

9 To import a **root CA certificate**, do the following:

- **a** Right-click **Trusted Root Certification Authorities**. This opens a shortcut menu.
- **b** Point to **All Tasks**, then select **Import...**. This opens the **Certificate Import Wizard**.
- **c** Click **Next**.
- **d** Click **Browse...**. This opens the **Open** dialog.
- **e** In the file filter box, select **X.509 Certificate (*.cer;*.crt)**.
- **f** Select the CER certificate and click **Open**.
- **g** Click **Next**.
- **h** Click **Next**.
- **i** Click **Finish** and confirm the success message.

10 To import an **intermediate CA certificate**, do the following:

- **a** Right-click **Intermediate Certification Authorities**. This opens a shortcut menu.
- **b** Point to **All Tasks**, then select **Import...**. This opens the **Certificate Import Wizard**.
- **c** Click **Next**.
- **d** Click **Browse...**. This opens the **Open** dialog.
- **e** In the file filter box, select **X.509 Certificate (*.cer;*.crt)**.
- **f** Select the CER certificate and click **Open**.
- **g** Click **Next**.
- **h** Click **Next**.
- **i** Click **Finish** and confirm the success message.

Appendix B
Licensing

About Open Text Auto Pass

Open Text Auto Pass is the licensing tool used with Dimensions RM and many other Micro Focus products. Auto Pass provides a web interface which allows administrators to manage licenses with ease.

If you intend to permanently install Dimensions RM rather than install it for just the default 30-day evaluation period, you will need to pre-install Auto Pass and provide its server name or IP address during Dimensions RM installation (however, if you wish to convert an evaluation copy of Dimensions RM into a fully licensed copy, you can install Auto Pass at a later date).

You can install Auto Pass on the same system as Dimensions RM or install it on a separate dedicated license server. If you have other Micro Focus software products installed on a license server that uses Auto Pass, you can use that for your Dimensions RM licenses.

For installation instructions see the https://docs.microfocus.com/itom/AutoPass_License_Server:latest/Home.

There is minimal CPU usage required on the server to run Auto Pass.

IMPORTANT! Ensure that **port (default 5814)** is open on the Auto Pass server.

Licensing Considerations

Install Micro Focus Auto Pass on a central server to which all related Micro Focus products will have access. See the related Auto Pass installation guide for instructions.
For supported Auto Pass versions please check the support matrix file in the following location: https://www.microfocus.com/documentation/dimensions-rm/

If licensing users in multiple locations with relatively slow networks, you may want to install an Auto Pass server for users in each location. However, faster networks, allow the installation and administration of Auto Pass from a single central server.

IMPORTANT! There should **NOT** be a firewall or router between the Auto Pass server and the RM server.

If that configuration is not possible and/or your network is slow, install Auto Pass and RM to the same server.

About Dimensions RM Licenses

To use Dimensions RM, you must generate and apply license keys. The following table explains the type of license keys that you can obtain and apply for each component:

License Type	Description
Concurrent	Concurrent licenses, also known as floating licenses, can be used by any user. This is advantageous if you are in an organization spread across multiple time zones or have users who infrequently use Dimensions RM, because multiple people can share the same license.
Named	Named licenses can only be used by specific users. This allows you to limit access to the system to only those users whose login IDs are associated with licenses.

Each RM license purchase comprises a license for the RM Browser client, RM Import, Class Definition, and web service requests.

This allows each RM license to be used simultaneously across multiple clients. For example. if there is just one available license, a user will be able to log into both RM Browser and RM Manage, without using multiple licenses.

The nature of the requirements process is best served with concurrent licenses, as there are peaks and valleys along the application lifecycle time line during which different teams will require access to the solution; however it is typical for organizations to maintain at least two named licenses. The general use case for these licenses is to assign them to administrator accounts, thereby ensuring administrator access if all concurrent licenses are in use.

In the general case, named licenses should only be purchased for full time analysts - individuals spending 25-30 hours a week in RM or for the Web Service service account to ensure that the Web Service connections are always served with a license.

After Setting Up the Licenses

After getting and setting up licenses, you are ready to start using Dimensions RM with Micro Focus Auto Pass. If you have not already done so, proceed with installing Dimensions RM (see chapter "Installation Types" on page 52). Make sure that the users responsible for installing Dimensions RM know the name or IP address of the Auto Pass server so they can successfully complete their Dimensions RM installation.

Appendix C

Installing and Configuring Oracle

Overview

Dimensions RM can use a database from Oracle, Microsoft SQL Server, or PostgreSQL. This chapter describes how to install and configure Oracle. For installing and configuring Microsoft SQL Server, see chapter "Installing and Configuring MS SQL" on page 139. For installing and configuring PostgreSQL, see chapter "Installing and Configuring PostgreSQL" on page 147.

Oracle System Requirements

Supported Oracle Versions

The Dimensions RM server requires database connectivity to one of the following supported RDBMS (in which it locates its databases):

IMPORTANT! For the list of currently supported RDBMS platforms, chip architectures, operating-systems, Web servers, Web browsers, and Micro Focus and third-party integrations, see the Dimensions RM Platform Matrix on the Support Download page:

https://www.microfocus.com/documentation/dimensions-rm/

NOTE The Dimensions RM server and the Dimensions RM Admin tools are 64-bit applications and require a 64-bit Windows platform to run. RM Import can run on either a 32-bit or 64-bit Windows platform.

- A 64-bit Windows Oracle Standard or Enterprise located on either the same network node as the Dimensions RM server or a remote network node.
- A 64-bit UNIX Oracle Standard or Enterprise. This can only be located on a network node remote from the Dimensions RM server.

For supported Oracle versions please check the support matrix: https://www.microfocus.com/documentation/dimensions-rm/.

The Administrator Oracle Client

A 64-bit Oracle Administrator Client, supported by the release level of the RDBMS must be installed if any of these conditions is met:

- You are installing Dimensions RM server **and** the database is installed on a remote machine
- You are installing on a separate web server **and** the database is installed on a remote machine
- You are installing Dimensions RM Admin tools on a client machine

If none of the above conditions matches, **do not** install the Oracle client.

NOTE

- If you have a 64-bit Oracle installed on the same machine as Dimensions RM, you should check to see whether the 64-bit Oracle client components are installed by attempting to connect to the database using sqlplus. Install a 64-bit Administrator Oracle client if the connection test shows that it is currently absent.
- The release levels of the Oracle client must match that of the RDBMS.
- The 64-bit client path must be first in the Windows PATH variable.
- RM Import Client does not require the Oracle client (it communicates to Dimensions RM via Web services).

TIP Oracle provides a client only install. You do not need to do another server installation to obtain the 64-bit Oracle Administrator Client.

About Containers

Oracle introduced the term container database (CDB) with database release 12c. A non-CBD refers to any database created before 12c, or a (12c or higher) database created without the enable pluggable database clause.

Configuring Oracle

If upgrading to a newer release of RM on a server previously hosting RM, you may proceed directly to Chapter E, "Upgrading an Earlier Release of Dimensions RM" on page 99.

NOTE This applies to Oracle ASM users:
Do not use an ASM controlled folder (ASM folders begin with a '+') for backup or for restore. A standard operating system path must be used from RM Manage to backup and restore operations.

Microsoft Loopback Adapter For a Windows RDBMS

Many Windows networked systems implement Dynamic Host Configuration Protocol (DHCP) to assign dynamic IP addresses on a computer network. Dynamic addressing allows a computer to have a different IP address each time it connects to the network. This simplifies network administration by letting you add a new computer to the network without having to manually assign that computer a unique IP address.

The Window versions of the Oracle RDBMS, however, require a static IP address. On a DHCP network, the assignment of a static IP address can be achieved by installing a Microsoft Loopback Adapter as the primary adapter. If this is not installed, whenever the DHCP-assigned IP address subsequently changes (for example, at a system reboot), the Oracle Net Listener will no longer work and will have to be recreated using the Oracle Net Configuration Assistant tool.

For instructions on how to install the Microsoft Loopback Adapter, please refer to the Oracle documentation.

Creating the Oracle Database Instance for RM

If there are any questions as you proceed through this setup, please contact Micro Focus Support – they will be happy to assist.

The following is the short answer to the question: "How do I create a database instance for RM?" For additional detail, please refer to The Database Instance Creation Details, below.

1. Begin by using Oracle Database Configuration Assistant option to 'Create a Database'.
2. Select the template for a General Propose or Transaction Processing Template.
3. Use Default settings with the following exceptions:
   - **a** Memory tab: Enable Automatic Memory Management with at least **2GB** of memory.
   - **b** Sizing Tab: Increase Processes from 150 to a minimum of 310.
   - **c** Character sets:
     - NLS_Characterset AL32UTF8
     - NLS_NCHAR_Characterset AL16UTF16
   - **d** Connection must be DEDICATED.

The Database Instance Creation Details

NLS_CHARACTERSET

NLS_CHARACTERESET	Supported/Unsupported
US ASCII	Unsupported
WE81SO8859P1	Supported
AL32UTF8	Supported
UTF8	Unsupported
Double-byte	Unsupported

NLS_NCHAR_CHARACTERSET

NLS_NCHAR_CHARACTERSET	Supported/Unsupported
US7 ASCII	Unsupported
AL16UTF16	Supported
UTF8	Supported
Double-byte	Unsupported

NLS_LANGUAGE

NLS_LANGUAGE	Supported/Unsupported
American	Supported
All Others	Unsupported

Oracle Client - NLS_LANG (Windows Registry Setting)

NLS_LANG	Supported/Unsupported
AMERICAN_AMERICA. WE8MSWIN1252	Supported
All Others	Unsupported

Local Windows Clients Character Set Encoding

	Supported/Unsupported
Western European (English on English Windows Operating System)	Supported
Western European (English on French Windows Operating System)	Supported
Western European (English on German Windows Operating System)	Supported
All Others	Unsupported

Browser Character Set Encoding

	Supported/Unsupported
UTF8	Supported
Windows	**Supported**
All Others	Unsupported

Memory Management–32 Bit

NOTE The following values are not minimum values for Oracle operations but recommended starting points. If you have an Oracle DBA, they should tune these values until they achieve optimum performance for the actual data stored in the Dimensions RM database.

The users referred to in the computations are users simultaneously accessing the server for information.

Attribute	Value to be Set
Shared Memory Management	AUTOMATIC
SGA size	768MB plus 48MB for each simultaneous user over four users
PGA size	256MB plus 16MB for each simultaneous user over four users

Attribute	Value to be Set
1-4 simultaneous users SGA/PGA	SGA 768MB; PGA 256MB
5 simultaneous users SGA/PGA	SGA 1056MB; PGA 272MB
10 simultaneous users SGA/PGA	SGA 1536MB; PGA 352MB
20 simultaneous users SGA/PGA	SGA 1536MB; PGA 512MB

Memory Management–64 Bit

NOTE The following values are not minimum values for Oracle operations but recommended starting points. If you have an Oracle DBA, they should tune these values until they achieve optimum performance for the actual data stored in the Dimensions RM database.

The users referred to in the computations are users simultaneously accessing the server for information.

Attribute	Value to be Set
Shared Memory Management	AUTOMATIC
SGA size	1152MB plus 64MB for each simultaneous user over eight users
PGA size	384MB plus 32MB for each simultaneous user over eight users
1-8 simultaneous users SGA/PGA	SGA 1152MB; PGA 384MB
10 simultaneous users SGA/PGA	SGA 1280MB; PGA 448MB
20 simultaneous users SGA/PGA	SGA 1920MB; PGA 768MB

Processes

NOTE For most systems, 310 processes are adequate; but for large systems a greater number of processes are required. For large systems, if you have an Oracle DBA, they should tune these values until they achieve optimum performance for the actual data stored in the Dimensions RM database.

Category	Number of Processes
Each simultaneous user	At least eight
Each sync engine	At least 20
Each ALF or Mashups service	At least 18
Each RM Mail Service	At least four
All categories	A minimum of 768 (must be a multiple of 32)

64-Bit Oracle Client Installation in an Upgrade Scenario

You must install the 64-bit Oracle client if any of these conditions is met:

- You are installing Dimensions RM server **and** the database is installed on a remote machine
- You are installing on a separate web server **and** the database is installed on a remote machine
- You are installing Dimensions RM Admin tools on a client machine

Please note that the Oracle client version and patch level must be supported by the server.

1. Run the Oracle client install (setup.exe) as Administrator, **choosing installation type Administrator**.
2. From your backup, copy the tnsnames.ora file to …\64bitClient\product\<version_number>\client_1\network\admin
3. **Set the PATH environment variable such that the 64-bit client path appears first in the system PATH variable**. This path-setting is necessary for a successful RM installation.

64-Bit Oracle Client Installation with a Fresh Installation

You must install the 64-bit Oracle client if any of these conditions is met:

- You are installing Dimensions RM server **and** the database is installed on a remote machine
- You are installing on a separate web server **and** the database is installed on a remote machine
- You are installing Dimensions RM Admin tools on a client machine

Please note that the Oracle client version and patch level must be supported by the server.

1. Run the Oracle client install (setup.exe) as Administrator, **choosing installation type Administrator**.
2. Configure tnsnames.ora
   a. Copy tnsnames.ora file from server to Oracle client install path
   For example, from
   …\Oracle_install\NETWORK\ADMIN\tnsnames.ora
   To
   …\64bitClient\product\<version_number>\client_1\network\admin\tnsnames.ora
   b. For the client's tnsnames.ora file and a container database, add**:**

```
CONTAINER_NAME =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = hostname)(PORT = 1521))
    (CONNECT_DATA =
      (SERVER = DEDICATED)
```

```
        (SERVICE_NAME = CONTAINER_NAME)
    )
  )
```

NOTE

- Replace ***CONTAINER_NAME*** with the actual name of the container. To retrieve a list of containers in your database, see chapter "Listing Containers in an Oracle database" on page 134.
- After configuration of the container in the client's TNSnames file (and restarting RM Manage), the container name will show like a database entry in RM Manage. Any operation which is usually executed on the database has to be executed with the container, e.g.
  - Creating the ICDBA account
  - Creating RM instances
  - Accessing RM instances

3 **Set the PATH environment variable such that the 64-bit client path appears first in the system PATH variable**. This path-setting is necessary for a successful RM installation.

Listing Containers in an Oracle database

The following steps assume the database connection name RTM. If your database connection name (in the tnsnames.ora file of your Oracle Client) is different, use that name instead.

To list all containers in the database:

1 Open a command prompt.

2 Type the following command and press **Enter**: `sqlplus`

3 Enter the following user name and press **Enter**: `sys@RTM as sysdba`

4 Type the password and press **Enter**. Note that there is no graphical representation for the password characters on the screen.

5 Type the following command and press **Enter**: `column name format A8`

6 Type the following command and press **Enter**:
`select NAME, CON_ID from V$CONTAINERS order by CON_ID;`

7 To close the connection to the database, type the following command and press **Enter**: `exit`

EXAMPLE

This example uses the database name "rtm". Replace this with the actual name of your database.

```
C:\>sqlplus

SQL*Plus: Release 12.1.0.1.0 Production on Wed May 13 11:04:10 2020

Copyright (c) 1982, 2013, Oracle.  All rights reserved.

Enter user-name: sys@rtm as sysdba
Enter password:

Connected to:
Oracle Database 12c Enterprise Edition Release 12.1.0.1.0 - 64bit
    Production

With the Partitioning, OLAP, Advanced Analytics and Real Application
Testing options

SQL> column name format A8
SQL> select NAME, CON_ID from V$CONTAINERS order by CON_ID;

NAME         CON_ID
-------- ----------
CDB$ROOT          1
PDB$SEED          2
ORCLPDB           3

SQL> exit
```

With this example, the container name is *ORCLPDB*.

Preparing an existing Container for Dimensions RM

To allow Dimensions RM to use the container, it must have the status **OPEN**. The following steps assume the container name ORCLPDB and user sys. Change these according to your environment.

To prepare a container:

1 Open a command prompt.

2 Type the following command and press **Enter**: `sqlplus`

3 Enter the following user name and press **Enter**: `sys@ORCLPDB as sysdba`

4 Type the password and press **Enter**. Note that there is no graphical representation for the password characters on the screen.

5 Type the following command and press **Enter**:
`select STATUS, DATABASE_STATUS from v$instance;`

6 If the STATUS column shows **OPEN**, continue with step 10.

7 Type the following command and press **Enter**: `alter database open`

8 Type the following command and press **Enter**:
`select STATUS, DATABASE_STATUS from v$instance;`

9 Verify that the STATUS column shows **OPEN**.

10 To close the connection to the database, type the following command and press **Enter**: `exit`

Completing the Oracle Configuration

Turning Off the Anonymous User

The way in which Oracle authenticates your anonymous user may prevent you from connecting to the database. If the anonymous user does not exist in the domain, turn the authentication service off in Oracle. To do this, modify the `sqlnet.ora` file in the `network\admin` directory as described:

Change:

```
SQLNET.AUTHENTICATION_SERVICES=(NTS)
```

to:

```
SQLNET.AUTHENTICATION_SERVICES=(NONE)
```

NOTE This problem can occur when you attempt to populate the Instances list on the RM Browser login page.

Setting Up a Local Oracle Net Service Name on the Dimensions RM Server Node

For a Dimensions RM server installation with respect to a supported remotely located Oracle RDBMS, you will need to provide the Oracle Net Service Name. This is the name that the local Windows Oracle client networking software uses to identify particular remote Oracle databases for network operations.

On your local Windows node you need to define the Net Service Name of the remote Oracle database that you want the Dimensions RM server to communicate with. To do this you use the Oracle Net Configuration Assistant as explained below:

1 Start the Oracle Net Configuration Assistant.

2. Select **Local Net Service Name configuration** and click **Next**.

3. Select **Add** and click **Next**.

4. Each Oracle database or service has a service name. Normally this will be its SID. Enter the SID of the *remote* database you want the *local* Oracle client to communicate with and click **Next**.

5. Select **TCP** and click **Next**.

6. To be able to communicate with the remote database, the local Oracle client needs to know the remote database's hostname. Enter the remote database's hostname. (In most cases you should also accept the standard port number of 1521.) Click **Next**.

7. Select **Yes, perform a test** to verify that the remote database can be reached using the information already provided. Click **Next**.

8. If the test was successful, you will get the message:

   ```
   Connecting... Test successful.
   ```

   If the test fails, you need to repeatedly click **Back** to check that the information you provide and correct it as necessary until this test is successful.

   Click **Next**.

9. Having tested that your local Oracle client can simply communicate through TCP/IP with the remote database whose service name (SID) you provided in Step 4 on page 137, you now need to assign an Oracle Net Service Name. This net service name is the name that your *local Oracle client* will use to identify the *remote* database when performing locally initiated Oracle services with respect to the *remote* database.

   By default the net service name will be the same as the service name you provided in Step 4 on page 137 and the **Net Service Name** field will be pre-populated with that name. However, if that name is not unique, for example, say both the local Oracle client and remote databases have an Oracle SID of `DIM10`, then you would enter a unique net service name for the local Oracle client to use when communicating with the remote database, for example, `DIM10R`.

   Click **Next**.

10. Unless you want to configure another net service name, accept the default **No** and click **Next**.

11. Click **Next**.

12. Click **Finish**.

Appendix D

Installing and Configuring MS SQL

Overview

Dimensions RM can use a database from Oracle, Microsoft SQL Server, or PostgreSQL. database. This chapter describes how to install and configure Microsoft SQL Server. For installing and configuring Oracle, see chapter "Installing and Configuring Oracle" on page 127. For installing and configuring PostgreSQL, see chapter "Installing and Configuring PostgreSQL" on page 147.

MS SQL Server System Requirements

The Dimensions RM server requires database connectivity to one of the following supported RDBMS (in which it locates its databases):

IMPORTANT! For the list of currently supported RDBMS platforms, chip architectures, operating-systems, Web servers, Web browsers, and Micro Focus and third-party integrations, see the Dimensions RM Platform Matrix on the Support Download page:

https://www.microfocus.com/documentation/dimensions-rm/

NOTE The Dimensions RM server and the Dimensions RM Admin tools are 64-bit applications and require a 64-bit Windows platform to run. RM Import can run on either a 32-bit or 64-bit Windows platform.

- One of these Microsoft SQL Server releases:
  - MS SQL Server 2017 with cumulative update 25
  - MS SQL Server 2019
- A database instance which will receive the data of the Dimensions RM instances to be created.
- A 64-bit ODBC System DSN based on **SQL Server Native Client 11 drive**r must be installed on the Dimensions RM application server.

Installing SQL Server

IMPORTANT! For SQL Server, **Mixed Mode** must be enabled.

Mixed Mode allows to authenticate against SQL Server with domain user accounts and SQL Server user accounts. The following steps are guidelines for installing SQL Server based on the MS SQL Server 2017 setup. These guidelines are for reference only. Micro Focus may not be held liable for any damages resulting from these guidelines.

To install SQL Server:

1. Right-click **setup.exe** of SQL Server and select **Run as administrator** from the shortcut menu. This opens the **SQL Server Installation Center**.
2. Select **Installation** from the pane.

3 Click **New SQL Server stand-alone installation or add features to an existing installation**. This opens the SQL Server Setup wizard.

4 Enter the product key and click **Next**.

5 Select the **I accept the license terms.** option and click **Next**.

6 If desired, select the **Use Microsoft Update to check for updates (recommended)** option.

7 Click **Next**.

8 Click **Next**.

NOTE If the Windows Firewall is enabled, you may receive a warning. You should allow SQL Server access through the firewall if

- SQL Server is installed on a different server than Dimensions RM or
- you need to access SQL Server from another machine (e.g. by using Dimensions RM Admin tools or SQL Server Management Studio)

If none of the options above applies, you can ignore the message.

9 Select **Database Engine Services**.

10 Select any other feature you require or desire (optional).

11 Click **Next**.

12 Ensure that the **Default instance** option is selected.

13 If desired, specify a different **Instance ID**. If you do, take a note as the Instance ID is required for connecting to the database. The following chapters assume that you leave the default **MSSQLSERVER**.

14 Click **Next** twice.

15 Select **Mixed Mode (SQL Server authentication and Windows authentication).**

16 Enter a password for the sa account in the **Enter password** and **Confirm password** boxes. Take a note of the password.

17 Click **Next**.

18 Click **Install**.

19 After installation is complete, verify that all setup steps have the status **Succeeded**.

20 Click **Close**.

Configuring SQL Server

Before you can use SQL Server, you must configure the method how it can be accessed. There are two options: TCP/IP or Named Pipes. The following steps describe how to Enable TCP/IP and disable Named Pipes.

To configure TCP/IP for SQL Server, do the following:

1. From Windows Start menu, start the SQL Server Configuration Manager.
2. Expand **SQL Native Client 11.0 Configuration (32bit)**.
   a. Select **Client Protocols**.
   b. If **Named Pipes** is enabled, right-click **Named Pipes** and select **Disable** from the shortcut menu.
   c. If **TCP/IP** is disabled, right-click **TCP/IP** and select **Enable** from the shortcut menu.
3. Expand **SQL Server Network Configuration**.
   a. Select **Protocols for *MSSQLSERVER***. Note that you may see a different name than *MSSQLSERVER* if you changed the instance name during setup.
   b. If **Named Pipes** is enabled, right-click **Named Pipes** and select **Disable** from the shortcut menu.
   c. If **TCP/IP** is disabled, right-click **TCP/IP** and select **Enable** from the shortcut menu.
4. Expand **SQL Native Client 11.0 Configuration**.
   a. Select **Client Protocols**.
   b. If **Named Pipes** is enabled, right-click **Named Pipes** and select **Disable** from the shortcut menu.
   c. If **TCP/IP** is disabled, right-click **TCP/IP** and select **Enable** from the shortcut menu.
5. Select **SQL Server Services**.
6. Right-click **SQL Server (MSSQLSERVER)** and select **Restart** from the shortcut menu. Note that you may see a different name than *MSSQLSERVER* if you changed the instance name during setup.
7. When using MS SQL Server Express or you use more than one SQL Server instance, ensure that the **SQL Server Browser** service is running and started automatically by executing these steps:
   a. Select **SQL Server Services**.
   b. Double-click the **SQL Server Browser** service.
   c. Select the **Service** tab.
   d. Ensure that the **Startup Mode** shows **Automatic** and click **Apply** if you changed it.
   e. Select the **Log On** tab.
   f. Click **Start**.
   g. Click **OK**.

Installing SQL Server Management Studio

To allow easy management of Microsoft SQL Server, you might want to use SQL Server Management Studio. The following steps are guidelines for installing SQL Server Management Studio based on the Release 18.6 setup. These guidelines are for reference only. Micro Focus may not be held liable for any damages resulting from these guidelines.

1. Right-click the SQL Server Management Studio setup and select **Run as administrator** from the shortcut menu.
2. Click **Install**.
3. Click **Restart**.

Creating a Database Instance

CAUTION!

- When creating the database instance, always use an **SQL Server user account** e.g. the **sa** user account. **Do not** use a domain user account.
- You must only use 1 database instance for Dimensions RM per MS SQL Server installation.

To allow Dimensions RM to function, a database instance must be available to Dimensions RM. The following steps assume that SQL Server Management Studio has been installed. The following steps give a guideline for creating a database instance and are for reference only. Micro Focus may not be held liable for any damages resulting from these guidelines.

To create a database instance, execute these steps:

1. Start SQL Server Management Studio.
2. **Server type:** Select **Database Engine**.
3. **Server name:** If SQL Server is on a different machine, enter the server name or IP address of the server running SQL Server.
4. **Authentication:** Select **SQL Server Authentication**.
5. **Log in:** Type **sa**.
6. **Password:** Type the password for the **sa** user account.
7. Click **Connect**.
8. If required, expand the root node in **Object Explorer**.
9. Right-click the **Databases** folder and select **New Database...** from the shortcut menu. This opens the **New Database** dialog.
10. Enter a database name, e.g. ***RTM***.
11. Click **OK** to create the database.

Installing and Configuring the ODBC Driver

An ODBC driver for SQL Server, supported by the release level of the SQL Server must be installed in order to use the following Dimensions RM components:

- A Dimensions RM server communicating with a remote 64-bit SQL Server instance.
- A Dimensions RM server communicating with a local 64-bit SQL Server instance.
- A Dimensions RM Admin Client communicating with a Dimensions RM database.
- Web Server

NOTE RM Import Client does not require the ODBC data source (it communicates to Dimensions RM via Web services).

Installing the ODBC Driver for MS SQL Server for Separate Setups

Dimensions RM requires the 64-bit version of Microsoft® ODBC Driver 11 for SQL Server®. The following steps are guidelines for installing the MS ODBC Driver 11 for SQL Server and are for reference only. Micro Focus may not be held liable for any damages resulting from these guidelines.

IMPORTANT! If database SQL Server and Dimensions RM are installed on the same machine, proceed to "Configuring the System DSN" on page 145.

To install the ODBC driver for MS SQL Server 2017 CU 25 and higher, execute these steps:

1. Navigate to the support directory of your Dimensions RM setup (*X*:**\RM\win32\support** - Replace X with the letter of your DVD drive).
2. **Installing the MS ODBC Driver for SQL Server**
   a. Double-click `msodbcsql.msi`. This opens the **Microsoft ODBC Driver 13 for SQL Server Setup** dialog.
   b. Click **Next**.
   c. Select **I accept the terms in the license agreement** and click **Next**.
   d. Ensure that **Client Components** is selected (no red x) and click **Next**.
   e. Click **Install**.
   f. Click **Finish**.
3. **Installing the Microsoft Command Line Utilities 13 for SQL Server**
   a. Double-click `MsSqlCmdLnUtils.msi`. This opens the **Microsoft Command Line Utilities 13 for SQL Server Setup** dialog.
   b. Click **Next**.

c Select **I accept the terms in the license agreement** and click **Next**.

d Click **Install**.

e Click **Finish**.

4 Installing the Microsoft SQL Server 2012 Native Client

a Double-click `sqlncli.msi`. This opens the **Microsoft SQL Server 2012 Native Client Setup** dialog.

b Click **Next**.

c Select **I accept the terms in the license agreement** and click **Next**.

d Ensure that **Client Components** is selected (no red x) and click **Next**.

e Click **Install**.

f Click **Finish**.

Configuring the System DSN

A System DSN must be created to allow Dimensions RM to connect to the database.

To create a System DSN, execute these steps:

1 Open Windows Explorer and navigate to `C:\Windows\System32`.

2 Start `odbcad32.exe`.This opens the **ODBC Data Source Administrator (64-bit)** dialog.

3 Select the **System DSN** tab.

4 Click **Add...**. This opens the **Create New Data Source** dialog.

5 Select **SQL Server Native Client 11.0** and click **Finish**. This opens the **Create a New Data Source to SQL Server**.

6 Enter a connection name into the **Name** box. Note that the name must all be uppercase.

7 If desired, specify a description into the **Description** box.

8 In the **Server** box, specify the server by name or IP address.

9 Click **Next**.

10 Select option **With SQL Server authentication using a login ID and password entered by the user**.

11 Enter **sa** into the **Login ID** box.

12 Enter the password for the "sa" user into the **Password** box.

13 Click **Next**.

14 Select the **Change the default database** to option and enter the database instance you created, e.g. ***RTM***.

15 Click **Next**.

16 Click **Finish**.

17 Click **OK** to close the **ODBC Microsoft SQL Server Setup** dialog.

18 Click **OK** to close the **ODBC Data Source Administrator (64-bit)** dialog.

NOTE RM Import Client does not require the ODBC data source (it communicates to Dimensions RM via Web services).

Appendix E

Installing and Configuring PostgreSQL

Overview

Dimensions RM can use a database from Oracle, Microsoft SQL Server, or PostgreSQL. This chapter describes how to install and configure PostgreSQL. For installing and configuring Oracle, see chapter "Installing and Configuring Oracle" on page 127. For installing and configuring Microsoft SQL Server, see chapter "Installing and Configuring MS SQL" on page 139.

IMPORTANT! For the list of currently supported RDBMS platforms, chip architectures, operating-systems, Web servers, Web browsers, and Micro Focus and third-party integrations, see the Dimensions RM Platform Matrix on the Support Download page:

https://www.microfocus.com/documentation/dimensions-rm/

PostgreSQL System Requirements

NOTE The Dimensions RM server and the Dimensions RM Admin tools are 64-bit applications and require a 64-bit Windows platform to run. RM Import can run on either a 32-bit or 64-bit Windows platform.

- PostgreSQL release 13.x (64-bit), or 14.x (64-bit). Release 14.1 can be found in the `support` folder of your Dimensions RM setup.
- A database instance which will receive the data of the Dimensions RM instances to be created.
- A 64-bit System DSN which allows connection to PostgreSQL.

Installing PostgreSQL

PostgreSQL can also be installed by Dimensions RM setup. This however, installs PostgreSQL on the same machine as Dimensions RM.

To install PostgreSQL 14.1:

1. Navigate to the `support` directory of your Dimensions RM setup (*X*:**\RM\win32\support** - Replace X with the letter of your DVD drive).
2. Right-click **postgresql-14.1-1-windows-x64.exe** and select **Run as administrator** from the shortcut menu. This opens the setup wizard.
3. Click **Next**.
4. If desired, change the installation directory.
5. Click **Next**.
6. Ensure that all options are selected.
7. Click **Next**.

8 If desired change the data directory (which will receive the database files).

9 Click **Next**.

10 Specify the password for the database superuser (postgres) into the **Password** box.

11 Re-type the password in the **Retype password** box.

12 Take a note of the password.

13 Click **Next**.

14 Specify the port for the PostgreSQL database. By default, the port is `5432`.

15 Take a note of the port.

16 Click **Next**.

17 From the Locale, box, select **English, United States**.

18 Click **Next**.

19 Review your settings and click **Next**.

20 To install PostgreSQL, click **Next**.

21 After installation is complete, verify setup has been completed successfully.

22 Clear the **Launch Stack Builder at exit** option.

23 Click **Finish**.

IMPORTANT! Right after installation, Dimensions RM can access PostgreSQL only if it is on the same server. Be sure to execute the steps in chapter "Configuring PostgreSQL" on page 151.

Installing the PostgreSQL Command Line Tools

The PostgreSQL command line tools are required for Admin Client installations or if the PostgreSQL database is on a different machine.

Running the Setup for Installation of the PostgreSQL Command Line Tools

To install the PostgreSQL 14.1 Command Line Tools:

1 Navigate to the `support` directory of your Dimensions RM setup (*X*:**\RM\win32\support** - Replace X with the letter of your DVD drive).

2 Right-click **postgresql-14.1-1-windows-x64.exe** and select **Run as administrator** from the shortcut menu. This opens the setup wizard.

3 Click **Next**.

4 If desired, change the installation directory.

5 Click **Next**.

6 De-select the **PostgreSQL Server** option.

7 De-select the **pgAdmin** 4 option if you do not want to administer the database.

8 De-select the **Stack Builder** option.

9 Ensure that the **Command Line Tools** option is selected.

10 Click **Next**.

11 Review your settings and click **Next**.

12 To install the PostgreSQL Command Line Tools, click **Next**.

13 After installation is complete, verify setup has been completed successfully.

14 Click **Finish**.

Setting the Registry Key for Backup/Restore

When installing the Command Line Tools, PostgreSQL setup does not set a registry key, that is required by RM Manage to retrieve the location of PostgreSQL's bin folder.

Execute the following steps to create the registry entry:

1 Open Windows Registry editor (select **Run**, enter `regedit` and click **OK**).

2 Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE`.

3 Check, if the registry key `PostgreSQL Global Development Group` exists.

Registry key `PostgreSQL Global Development Group` does not exist:

a Right-click the **SOFTWARE** key and select **New | Key** from the shortcut menu. This adds a new key ready for changing the name as the last child to the **SOFTWARE** key.

b Type `PostgreSQL Global Development Group` and press **Enter**.

c Right-click the **PostgreSQL Global Development Group** key and select **New | Key** from the shortcut menu. This adds a new key ready for changing the name to the **PostgreSQL Global Development Group** key.

d Type `PostgreSQL` and press **Enter**.

e Right-click the **PostgreSQL** key and select **New | String Value** from the shortcut menu. This adds a new registry value ready for editing.

f Type `Location` and press **Enter**.

g Continue with step 7.

4 Expand the **PostgreSQL Global Development Group** key and check if the `PostgreSQL` key exists.

Registry key `PostgreSQL` does not exist:

a Right-click the **PostgreSQL Global Development Group** key and select **New | Key** from the shortcut menu. This adds a new key ready for changing the name to the **PostgreSQL Global Development Group** key.

b Type `PostgreSQL` and press **Enter**.

c Right-click the **PostgreSQL** key and select **New | String Value** from the shortcut menu. This adds a new registry value ready for editing.

d Type `Location` and press **Enter**.

e Continue with step 7.

5 Select the `PostgreSQL` key.

6 Check if the `Location` value exists. If the Location value does not exist, execute the following steps:

a Right-click the **PostgreSQL** key and select **New | String Value** from the shortcut menu. This adds a new registry value ready for editing.

b Type `Location` and press **Enter**.

7 Double-click the **Location** entry. This opens the **Edit String** dialog.

8 Enter the full path to the PostgreSQL directory into the Value data box.
Example: *`C:\Program Files\PostgreSQL\13`*.

9 Click **OK**.

Configuring PostgreSQL

Accessing PostgreSQL from other Machines

If the Dimensions RM server is installed on a different machine or you want the other applications (e.g. the Dimensions RM Admin tools) to connect to the database, you must configure PostgreSQL to allow that.

To allow access to PostgreSQL from other machines, do the following:

1 In Windows Explorer, navigate to the PostgreSQL data directory (default: `C:\Program Files\PostgreSQL\13\data`), which you specified during setup.

2 Open the `postgresql.conf` file with a text editor, e.g. Notepad.

3 Locate the `listen_addresses` setting.

4 Ensure that the `listen_addresses` setting has the value `'*'` assigned, so it looks like this:
`listen_addresses = '*'`
If it is not present, add it to the file.

5 Save the file.

6 Open the `pg_hba.conf` file, which is located in the same directory.

7 Scroll to the end of the file.

8 Add entries to specify the IP address of the machine or the IP address range you want to allow access for:

a Allow access to machine with IP address *`192.168.1.5`*:
`host all all` *`192.168.1.5`* `scram-sha-256`

b Allow access to all machines having an IP address with IP address *192.168.1.1* to *192.168.1.255*:
`host all all` *`192.168.1.1/24`* `scram-sha-256`

9 Save the file.

10 Start the **Services** console (`services.msc`).

11 Restart the PostgreSQL service (e.g. postgresql-x64-13).

Creating a Database Instance

To allow Dimensions RM to function, a database instance must be available to Dimensions RM. The following steps assume that pgAdmin has been installed with the PostgreSQL setup. The steps give a guideline for creating a database instance and are for reference only. Micro Focus may not be held liable for any damages resulting from these guidelines.

NOTE Dimensions RM supports only one PostgreSQL database instance per database server.

To create a database instance, execute these steps:

1 Start **pgAdmin**.

- **If you start pgAdmin for the first time:**
  - **a** Enter a password. This password is required whenever you start pgAdmin.
  - **b** Take a note of the password.
  - **c** Click **OK**.
- **If you started pgAdmin before:**
  - **a** Enter the password.
  - **b** Click **OK**.

2 Expand **Servers**. This opens the **Connect to Server** dialog.

3 Enter the password for the super user (which you defined during PostgreSQL setup).

4 Click **OK**.

5 Right-click **Databases**.

6 In the shortcut menu, point to **Create** and select **Database...**. This opens the **Create - Database** dialog.

7 Enter a database name, e.g. ***RM***.

8 Select the **Definition** tab.

9 Ensure that **Encoding** is **UTF8**.

10 Click **Save** to create the database.

Installing and Configuring the ODBC Driver

An ODBC driver for PostgreSQL, supported by the release level of the PostgreSQL must be installed in order to use the following Dimensions RM components:

- A Dimensions RM server communicating with a remote 64-bit PostgreSQL instance.
- A Dimensions RM server communicating with a local 64-bit PostgreSQL instance.
- A Dimensions RM Admin Client communicating with a Dimensions RM database.
- Web Server

NOTE RM Import Client does not require the ODBC data source (it communicates to Dimensions RM via Web services).

Dimensions RM requires the 64-bit version of PostgreSQL. The following steps are guidelines for installing the PostgreSQL Driver and are for reference only. Micro Focus may not be held liable for any damages resulting from these guidelines.

To install the ODBC driver for PostgreSQL, execute these steps:

1. Navigate to the `support` directory of your Dimensions RM setup (*X*:**\RM\win32\support** - Replace X with the letter of your DVD drive).
2. Double-click `psqlodbc_x64.msi`. This opens the **psqlODBC_x64 Setup** dialog.
3. Click **Next**.
4. Select **I accept the terms in the license agreement** and click **Next**.
5. Ensure that **Client Components** is selected (no red x) and click **Next**.
6. If desired install the documentation.
7. If desired change the target location:
   a. Click **Browse...**. This opens the Change destination folder dialog.
   b. Select the target directory into which you want to install the ODBC driver.
   c. Click OK.
8. Click **Next**.
9. Click **Install**.
10. Click **Finish**.

Configuring the System DSN

A System DSN must be created to allow Dimensions RM to connect to the database.

To create a System DSN, execute these steps:

1. Open Windows Explorer and navigate to `C:\Windows\System32`.
2. Start `odbcad32.exe`.This opens the **ODBC Data Source Administrator (64-bit)** dialog.
3. Select the **System DSN** tab.
4. Click **Add...**. This opens the **Create New Data Source** dialog.
5. Select **PostgreSQL Unicode(x64)** and click **Finish**. This opens the **PostgreSQL Unicode ODBC Driver (psqlODBC) Setup** dialog.
6. Fill out the following boxes:
   - **Data Source:** Enter a connection name. Note that the name must all be uppercase and must not contain spaces.
   - **Database:** Enter the database instance name (e.g. RM)
   - **Server:** Enter the server name or IP
   - **Port:** Enter the port on which to connect to the database (default: 5432).
7. If desired, specify a description into the **Description** box.
8. Click **Save** to close the **PostgreSQL Unicode ODBC Driver (psqlODBC) Setup** dialog.
9. Click **OK** to close the **ODBC Data Source Administrator (64-bit)** dialog.

NOTE RM Import Client does not require the ODBC data source (it communicates to Dimensions RM via Web services).

Index

Q

R

S

T

W