MICRO® FOCUS

Dimensions® RM 12.7.1
Installation Guide

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 12.7.1* of Dimensions RM*. This edition supersedes earlier editions of this manual.

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

License and copyright information for third-party software included in this release can be found as part of the software download available at:

http://support.serena.com/Download/Default.aspx

Chapter 1
Before Installing

Introduction

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 Serena License Manager (SLM).

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 11gR1 RDBMS. (*Note, Oracle 11gR1 is not supported on Windows Server 2008 R2*).

    - Oracle 11gR2 RDBMS.

    - Oracle 12c

    - Oracle 18c

  - **Microsoft:**

    - MS SQL Server 2016 SP1

- A pre-installed Serena License Manager (SLM). The installation instructions for this product are provided in the related *Installing the Serena License Manager* guide.

- Pre-installed Microsoft Office (32-bit). For details, see chapter "Microsoft Office Requirements" on page 19.

- 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 help with these 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 Platforms Web site:

http://nadownloads.microfocus.com/websync/
Internap_Download.aspx?FilePath=/serena/platformmatrix/
dimensionsrm/rtm_12.7.1.xlsx

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

- **UNIX RDBMS** must be installed on a remote UNIX network node.

- **For Oracle databases:**

  - **Oracle Administration Client:** You need to pre-install a supported 32-bit Administrator Oracle Client in a different Oracle Home 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 (because this uses the Oracle Call Interface).

    - "Fat" (non-browser) Dimensions RM Windows clients (because these use the Oracle Call Interface).

NOTE

- If you have a 32-bit Oracle installed on the same machine as Dimensions RM, you should check to see whether the 32-bit Oracle client components are installed by attempting to connect to the database using sqlplus. Install a 32-bit Oracle Administrator client if the connection test shows that it is currently absent.

- If you have a 64-bit Oracle installed on the same machine as Dimensions RM, you will need to install an additional 32-bit Oracle "Fat" Dimensions RM Windows client (because these use the Oracle Call Interface).

- The release level of the Oracle Administrator client must match that of the RDBMS.

- The 32-bit client path must be first in the Windows PATH variables.

- RM Import Client does not require the Oracle Administrator client (it communicates to Dimensions RM via Web services).

- The type of Oracle client required is Administrator (required for the Dimensions RM import/export functionality).

- The Oracle 11gR1 Administrator Client is not supported on Windows Server 2008 R2 or Windows 7.

See .

- **For Microsoft SQL Server:**

  - **32bit ODBC System DSN:** You need to set up a 32bit 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.

    - "Fat" (non-browser) Dimensions RM Windows clients (because these use the Oracle Call Interface).

    - Web Server.

- **Serena License Server:** You must pre-install the Serena License Manager (SLM) if you wish, by default, to fully license your installation of Dimensions RM, rather than exercise the 30-day evaluation option. See the *Installing Serena License Manager* guide and "Licensing Dimensions RM" on page 23.

- **Web Server:**

  - The Web server must be installed on a Windows machine.

  - When using Oracle databases, a 32-bit Oracle Administrator client must be installed on the same machine as the Web server. For a 64-bit Oracle, you will, however, normally have to also install a 32-bit client on the Web server machine.

- **RAM/CPU/Disk-Space Recommendations:** See the Readme.

- **Microsoft Office (32-bit):** Including .NET Programmability Support, must be installed on the Dimensions RM server to support browser-based Word import, Document Publishing, RM Import, and RM Import Designer tools. Note the following:

  - A message warns you if you do not have Office installed on your computer.

  - For consistent and reproducible use of the Document Publishing, RM Import and RM Import Designer tools, it is advisable to ensure that all users use the same version of Microsoft Office.

  - If you import requirements using the Word import feature in the RM Browser client, a supported 32-bit edition of Microsoft Office must be installed on the server to correctly import graphics from Word documents.

  - To be able to view Microsoft Word OLE-linked or embedded attachments when using Dimensions RM Document Publishing, the Windows user concerned must have been assigned administrator rights. This is a general Microsoft Word pre-requisite for utilizing OLE-linked or embedded attachments.

For further information, see chapter "Microsoft Office Requirements" on page 19.

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.

Pre-Installation / Planning Checklist

✓	Checklist Item
	Supported architectures, Web browsers, Databases, etc. For a list of all of the supported server architectures, Web browsers, Databases, etc., please see the Platform Matrix at <u>http://nadownloads.microfocus.com/websync/Internap_Download.aspx?FilePath=/serena/platformmatrix/dimensionsrm/rtm_12.7.1.xlsx</u>
	RAM / CPU / Disk-Space Recommendations For recommendations on RAM, CPU power, or Disk space, see the Dimensions RM Readme file.
	Serena License Manager and RM Licenses: First Time Install If installing a fully licensed release of Dimensions RM, install Serena License Manager (SLM) version 2.3.0 - before installing Dimensions RM. For evaluations there is a 30-day license option that may be selected during RM installation. See the *Installing Serena License Manager* guide and chapter "Licensing Dimensions RM" on page 23 in the *Dimensions RM Installation Guide*.
	Named Web Service License If Dedicated Service accounts are used for Web Services, vs SSO or changing user accounts, a Named License is recommended to ensure a lack of a license does not cause a failure.
	Downloading the 12.7.1 release of Dimensions RM 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: <u>http://supportline.microfocus.com</u>
	Oracle only: 32-bit Oracle Administrator Client on Application Server An Oracle 32-bit Admin Client must be installed on the Dimensions RM application server. Additional information can be found in chapter "The Administrator Oracle Client" on page 34. When executing the RM installation: **the Oracle client path must be first in the Windows PATH variable.** **Do *not* install the** 32-bit Oracle client into the default 32-bit Windows programs directory: `C:\Program Files(x86)`
	Oracle only: 32-bit Oracle Administrator Client on Web Server The Web server uses a 32-bit Oracle Call Interface (OCI) to communicate with Dimensions RM; therefore, a 32-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.

	MS SQL Server only: Database instance has been created A database instance on SQL server has been created.
	MS SQL Server only: 32-bit ODBC System DSN on Application Server A 32-bit ODBC System DSN based on SQL Server Native Client 11 driver must be installed on the Dimensions RM application server.
	MS SQL Server only: 32-bit ODBC System DSN on Web Server A 32-bit ODBC System DSN based on SQL Server Native Client 11 driver must be installed on the same machine as the Web server.
	Web Server must be Windows The Web server must be installed on a Windows machine.
	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.
	Server Host Names The host names of the server computers hosting the database and the Serena License Manager (SLM) 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.
	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.
	32-bit Microsoft Office Microsoft Office must be installed on the Dimensions RM server to support browser-based Word import, Document Publishing, RM Import, and RM Import Designer tools. For further information, see chapter "Microsoft Office Requirements" on page 19.
	Tomcat RM releases 12.1 and later install with Tomcat. Please check the following: **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.
	Planning your Dimensions RM user names and Passwords. If this is the first time Dimensions RM will be installed, you should plan for your Dimensions RM user names and define a strategy for managing their passwords, especially those for the ICDBA, ICADMIN, and ICPROJECTS accounts. If this is an update, please make sure that you are aware of these passwords.
	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.

	Installation folders: All examples in this document assume that Dimensions RM will be installed in: C:\Program Files (x86)\Micro Focus\Dimensions 12.7.1\RM Early in the installation process an option is provided to change the default location.
	Setting RM Instance passwords to not expire. Once Dimensions RM has been installed and configured, it is important to make sure that the Oracle passwords which were created for the ICDBA, ICADMIN, and ICPROJECTS accounts will not expire. In Oracle, the passwords will expire after 6 months by default. The section "Password Expiration for Oracle Passwords" in Chapter 5 of the *Dimensions RM Installation Guide* talks about this and provides an example SQL script to set the passwords so they don't expire.

Additional Plans for Upgrade

✓	Checklist Items for Users Upgrading from a Previous Release
	Upgrading the Serena License Manager If upgrading from a previous release of Dimensions RM, please be aware that **you must** upgrade the Serena License Manager to (SLM) to 2.3.0. RM Release 12.7.1 will not function with an older license manager. See the *Installing Serena License Manager* guide and chapter "Licensing Dimensions RM" on page 23 in the *Dimensions RM Installation Guide*.
	Installing the New Release Strictly speaking, there is no "upgrade" mechanism for Dimensions RM; that is to say the instances – the requirement data – will be upgraded to the new release, but the application itself. If this is not the initial installation of RM, **the older version must be uninstalled** before 12.7.1 can be installed. Before initiating the un-install procedure, copy the following from the current installation tree ■ The RM folder ■ The rtmBrowser folder, if running a release earlier than 12.x this folder will be included with the RM folder backup.
	Must start with 12.2 or later The earliest supported release for an upgrade of Dimensions RM is 12.2. ■ **Earlier than 12.2:** If the current version of Dimensions RM is earlier than 12.2, the release must first be upgraded to 12.2. ■ **Earlier than 11.2.4.2a:** If the current version of Dimensions RM is earlier than 11.2.4.2a, the release must first be upgraded to 11.2.4.2a and then to 12.2. Continue with the upgrade to 12.6 only after your Dimensions RM release is version 12.2 or later. For the upgrades to 12.2 or 11.2.4.2a refer to the documentation of the related release.
	Oracle only: 32-bit Oracle Administrator Client on Application Server An Oracle 32-bit Admin Client must be installed on the Dimensions RM application server. Additional information can be found in "The Administrator Oracle Client" on page 34. When installing RM - including with the upgrade: **the Oracle client path must be first in the Windows PATH variable.** **Do *not* install the** 32-bit Oracle client into the default 32-bit Windows programs directory: `C:\Program Files(x86)`
	MS SQL Server only: 32-bit ODBC System DSN on Application Server A 32-bit ODBC System DSN based on SQL Server Native Client 11 driver must be installed on the Dimensions RM application server.

	Dimensions RM User Names and Passwords. Before initiating the re-installation, make sure that you know the passwords for the ICDBA, ICADMIN, and ICPROJECTS accounts. If these three passwords are not known to you or to a member of the RM team, then re-set them before moving forward with the install.
	If the current release is configured to use RM Mail, see chapter "Record the Dimensions RM Mail Configuration" on page 101.
	Schedule RM Work Stoppage 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.
	Completing Your Installation Once the installation process has finished, the database and instances must be converted/upgraded to the new release. Please pay careful attention to the conversion steps.

Pre-Installation 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 "Pre-Installation / Planning Checklist" on page 14.

- The host names of the server computers that will host the database and the Serena License Manager (SLM) 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.

- 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 edition of Microsoft Office 2019, 2016, 2013, 2010 SP1 or newer including .NET Programmability Support is installed on the Dimensions RM server to support Document Publishing, RM Import and RM Import Designer tools. For further information, see chapter "Microsoft Office Requirements" on page 19.

■ 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 you install Dimensions RM. Please see "Installing and Configuring Your RDBMS and Database Client" on page 33.

Oracle 12 Requirements

■ Before installation, make sure that the system drive on your computer has default share configured on it. Use the net use command to verify, for example:
  `C:\>net use \\hostname\c$`
  Sending this command should return: `The command completed successfully.`

■ Ensure that the current user, the user in the Administrators group, has all the privileges on the default share.

Please follow the following link 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 32-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`

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:

■ DOCX format is not available for publishing. Documents publish to DOC instead.

■ PDF format is not available for publishing. Documents publish to DOC instead.

■ When publishing to Microsoft Word, the Table of Contents shows page 1 for all chapters.

■ Attachments cannot be published.

■ Import of Word or Excel files through RM Browser is not available.

■ Export of dashboards to PowerPoint is not available.

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

- The 32-bit edition of Microsoft Office, including .NET Programmability Support, must be installed.

- Microsoft Office must be any of these versions:

  - Microsoft Office 2019

  - Microsoft Office 2016

  - Microsoft Office 2013

  - Microsoft Office 2010 SP 1 or newer

- You must install Microsoft Word, Microsoft Excel, and Microsoft PowerPoint.

SSO Considerations

Support for Single Sign On requires either an SSO-enabled Micro Focus Solution Business Manager (SBM) or Dimensions CM server installation.

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** you 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.

General 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 Serena 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
Licensing Dimensions RM

About Serena License Manager

The Serena® License Manager (SLM) is the tool you use to obtain and apply the keys that unlock Dimensions RM. SLM enables you to centralize your license management across multiple Dimensions RM environments. SLM can help you keep track of active licenses and versions of the software in use, for example, you can use it to see whether or not all the licenses are in use or to manually track down who is using what version and license.

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 SLM 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 SLM at a later date). The SLM installer also installs the associated Serena License server.

You can install SLM on the same system as Dimensions RM or install it separately on a dedicated license server. If you have other Micro Focus software products installed on a license server that use a compatible version of SLM, for example Version Manager, you can use that with your Dimensions RM license. For installation instructions see the *Installing Serena License Manager* guide.

There is minimal CPU usage required on the server to run SLM.

License Manager Considerations

Install the Serena License Manager (SLM) on a central server that all related Micro Focus products will be able to access. See the related *Installing the Serena License Manager* guide for local or remote installation instructions. Dimensions RM release 12.7.1 requires the SLM release 2.3.0.

If you are licensing users in different locations and you have relatively slow networks, you may want to install a SLM server and set up the users in each location on the local server computer. When you do so, you need to install SLM to a server in each location. If you have faster networks, you can install SLM on one central network computer and have all Dimensions RM users point to it.

IMPORTANT! There should **NOT** be a firewall or router between the SLM server and the RM server.

If that configuration is not possible and/or your network is slow, install SLM 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 the following:

- icEWB license: A license for the client tools, such as RM Import.

- icPWB license: A license for RM Manage and Class Definition.

- icBrowser license: A license for the RM Browser client.

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.

The Licensing Process: Checklist

After downloading and installing Serena License Manager (SLM) version 2.3.0, you may proceed with "Web Fulfillment"; the process of accessing the license keys that will unlock the Dimensions RM product.

☐	Determine the number of Dimensions RM licenses you want to use in your organization.
☐	Contact your sales representative to purchase the licenses for your users or ensure that you have an existing Micro Focus Support contract.
☐	Ensure that you have a valid serial number for Dimensions RM.
☐	Ensure that you registered at the Micro Focus Support Web Site, in order to log in and get your license keys.

☐	Get the license key string from Micro Focus Web fulfillment.
☐	Enter the key string in Serena License Manager. Repeat this step if you have more than one serial number to license.
☐	*Named licenses only*: Manually set up user IDs if you do *not* want to use the auto-add feature to enter user IDs into SLM.
☐	Set up notification for licensing issues. If notification is enabled and there is a licensing issue, you will receive an e-mail detailing the problem.
☐	If you need to reboot the SLM server machine or set it to run as a service, restart the Windows SLM server (`Start | Programs | Micro Focus | SLM | Start License Manager Service`) or remote UNIX SLM server (run the `./start_license_server` script in the directory where you installed the license server).

Licensing Dimensions RM

Getting and Applying Licenses

To get a license from Micro Focus using SLM:

1 On Windows, open SLM by selecting `Start | Programs | Micro Focus | SLM 2.3.0 | License Manager`.

On remote UNIX, as user `root`, launch it by navigating to where you installed it and run the script:

`./serenalm`

> 📝 **NOTE** You must ensure that your UNIX search path environment includes the path to the license server process executable `lmgrd`. This executable is located in the directory where the Serena License Server is installed.

Then:

- If you already have a license key from Micro Focus, you can select the **I have received a license key** option and paste the key string in the field, then proceed to .

- If you don't already have a license key, select the **Connect to the web to get a license key** option on the Licensing tab and click the **Get Key(s)** button. The Micro Focus Support Licensing Web site login page appears.

2 To obtain the key from the Web fulfillment:

a Make sure, first, that you copy your license server host identity, which will be displayed in a "scissors" graphics.

b Click **Click here to continue >>**.

c Enter your Micro Focus Support account user name and password and log in. If you do not have a Micro Focus Support user name, you will need to register for one

using a valid serial number (if you do not have a valid serial number, contact Micro Focus).

d The Micro Focus Support Web page appears.

e Click the Licensing tab or navigate to the following menu item:

`Support | Licensing`

f Select appropriately from the (Licensing) **Site:**, **Product:**, **Serial Number:**, and **Version:** drop down menus.

g Click **Create Licenses** and follow the instructions presented there to obtain you license key or keys.

> **NOTE** If you require additional help, you can run an Adobe Flash video demo. Click the `View Demo` sub-tab.

h Once you have generated a license, electronically copy the entire license string and return to SLM. An e-mail will be sent to you with details of the license keys for your records.

> **IMPORTANT!** Make sure that you do not copy any extra spaces or SLM will consider the key invalid.

3 On return to the Serena License Manager, select the **I have received a license key** option and paste the keys (just the `FEATURE` lines) in the field available. The **Apply** button will then become active.

key string copied and pasted here

4 Click **Apply**. Your license will be activated. You can now:

- For any Named licenses that you added, add valid user IDs into the license server or set the license server to add in user names automatically before logging into Dimensions RM. See "Managing User Names for Named Licenses" on page 29.

- Set up notification for issues with the licenses and license server. See "Setting Up Notification for Licensing Issues" on page 29.

The license server on Windows will start automatically; if it does not, you can start it manually using Windows Services. On remote UNIX, you will need to start it manually in all cases. See "Starting the License Server" on page 28 for more information.

To get a license from Micro Focus if your server doesn't have Web access:

1   From a different computer with Web access, connect to the Micro Focus Support Web site. Make sure you know the product serial number and the Host ID of the license server machine so you can enter it in the Web fulfillment system.

You can find your license server machine's Host ID at the bottom of the **Licensing** tab of the Serena License Manager dialog box.

2   When you access the Web page with your key string, copy that key string into a text editor. Save and copy that file to a portable disk or a location on the network accessible from the license server machine.

3   Insert the portable disk in the license server machine or navigate to where the file is stored on the network. Open the file and copy the key string, select the **I have received a license key** option, and paste it in the field.

To get a license from Micro Focus if you don't have Web access at all:

Contact Micro Focus Support for assistance if you cannot use the Web to obtain a license. See "Contacting Technical Support" on page 8.

Adding Licenses

If all the licenses you purchased are not already in use, you can add license keys for seats you have already purchased through SLM.

If you run out of purchased license seats to use, contact your sales representative at Micro Focus to purchase additional licenses to add to your serial number.

To add license keys from your initial purchase:

1   Follow steps listed above in "To get a license from Micro Focus using SLM:" on page 26.

2   Click **Apply** to restart the license server.

To buy more licenses and add them to your pool of licenses:

Contact your Micro Focus sales representative to purchase additional licenses. Once you have your serial number updated for additional seats, follow the instructions above to obtain additional licenses.

Starting the License Server

If the license server did not start automatically after you have obtained the licenses, start it before installing other Micro Focus products.

On Windows   **To start and stop the license server:**

```
Start | Programs | Micro Focus | SLM 2.3.0 | Start License Manager
```

```
Service
```

To stop the license server:

```
Start | Programs | Micro Focus | SLM 2.3.0 | Stop License Manager
    Service
```

On UNIX   **To start the license server on UNIX:**

At a command prompt, as the Dimensions RM System Administrator user not `root` run:

```
<serena_license_server_dir>/<os>/start_license_server
```

where `<serena_license_server_dir>/<os>` is the directory in which you installed the Serena License Server, `<os>` being the platform identifier, for example, `aix`.

Check the contents of the `SLM.log` to make sure the service has started correctly.

To `stop` the license server:

At a command prompt, run:

```
<serena_license_server_dir>/<os>/stop_license_server
```

Managing User Names for Named Licenses

If you have purchased named user licenses, you need to specify the Dimensions RM user IDs and the features they are licensed to use in the SLM before that user can log into Dimensions RM. You can add the users' IDs manually by typing their user IDs or manually by accepting the default in the SLM.

To manually assign, reassign, or delete from features:

1   On the **Product** tab, select the feature from the **Product Licenses** list and click the **Manage User IDs** button.

2   The **User Management** dialog box opens.

- To add users manually, click **Add User** to add a user to the feature by typing in the user ID. You can add as many users as you like by separating the IDs with a space. The user names you enter here must match the users' Dimensions RM login names.

- To remove users from the list, select the user from the list and click **Remove User**.

To automatically assign named licenses to users who request them:

- On the Products tab, select the feature from the **Product Licenses** list and select **Auto-add user IDs for named licenses** to automatically add user IDs to a named license list when users log into Dimensions RM. This option is set by default.

    When users log in to a product, the server will check to see if there are licenses available for the feature they are attempting to use. If there is a license available, that user ID will be logged in the license server and that will be the named license assigned to the user.

Setting Up Notification for Licensing Issues

The **Notification** tab gives you the ability to set up notification from the license server. You need to supply the license server your SMTP server address and e-mail address to be notified of licensing issues by e-mail.

You can also suspend your notifications if the notices come in too frequently. It is also recommended that you set up rules in your e-mail application to funnel the incoming messages to an area where you can monitor them and where they won't interrupt your regular e-mail activity.

You can be notified of conditions such as when:

- You are out of licenses

- Users are requesting licenses that are not on the server

- Users are denied a license because they are not on the named list

To receive notification of license activity:

1 Enter your SMTP server address in the **SMTP Server IP / Hostname** field.

2 Enter your e-mail From address in the **From address** field.

3 Enter your e-mail To address in the **To address** field.

4 Click **Send e-mail notification of licensing issues** to enable notification.

5 Click **Apply Changes**.

To suspend notification of license activity:

To put notifications on hold, you can de-select **Send e-mail notification of licensing issues**. Select it again when you are ready to receive notifications.

Managing Your Licenses and the License Server

After you have installed SLM to obtain a license key for your users, you can later modify your SLM implementation, for example to run the SLM server as a service, or to move the SLM server.

Running the License Server as a Service

When the SLM installation is complete, the option to set the run the license server as a service is set by default. When the license server runs as a service the license server will restart automatically when you reboot the machine.

Should you need to stop and restart the service you do so in the lmtools utility.

To run the license server as a service:

On Windows **1** Go to the directory where you installed SLM and double click `lmtools.exe`.

2 Click the Config Services tab and select the **Use Services** check box. If you want the service to be automatic, select the **Start Server at Power Up** check box.

On UNIX If you are using the license server on remote UNIX, refer to the *FLEXlm User's Guide (enduser.pdf)* located in the `./doc/FLEXlm User's Guide` sub-directory of the directory where you installed SLM. This third-party document will guide you through the commands necessary for checking the server status and running it as a service.

Moving the License Server

If you need to move the license server to a new machine, you must contact Micro Focus Support for assistance. See "Contacting Technical Support" on page 8.

Upgrading from an Evaluation License

If you installed Dimensions RM and used an evaluation license, it is good for 30 days. After that period, you need to upgrade the evaluation license to a permanent license.

> **NOTE** You must perform this procedure *only* if you evaluated Dimensions RM without an SLM server. If you were already using SLM (for example, with an extended evaluation that included a temporary license key), all that you need to do is add the permanent license keys.

To upgrade to a permanent license:

1 Set up SLM and get a permanent license key.

2 In RM Manage, select **Options** from the **Workspace** menu.

3 Click the **License** tab.

4 Type the name of the license server in the **License Server** field.

5 Click **OK**.

Upgrading Your Serena License Manager

Dimensions RM 12.7.1 requires SLM Version 2.3.0. To upgrade from any previous version of SLM to this requirement version, please proceed as follows:

1 Shut down your existing version of SLM.

2 Back up the following files in the existing SLM installation directory:

- Windows
  - merant.opt (if you created such a file)
  - serena.lic
- UNIX
  - licmgr.ini
  - merant.opt (if you created such a file)
  - serena.lic
  - users.lst

3 Uninstall the existing SLM using **Add or Remove Programs** in the Control Panel.

4 Install the new version of SLM, see *Installing the Serena License Manager*.

5 Restore the files in Step 2 to the new SLM installation directory and start SLM.

Setting Up Redundant License Manager Servers

To help ensure that licenses are always available in case the SLM server fails, you can set up redundant SLM servers. In this scenario, if one of the servers fails or loses network connectivity, the remaining servers will still supply the licenses to users to ensure that they can log in.

To set up redundant servers, you must:

Request redundant server license keys from Micro Focus Support Sales.

Redundant server license keys enable special licenses that redundant servers can share. With these keys, each of the three servers shares common license information, enabling the servers to back each other up should one go down.

When you receive redundant server license keys, you also receive detailed instructions on how to set up the redundant servers and on how to install and use the keys.

Install the License Manager server to three separate systems.

These systems must have continuous, reliable, high quality network connectivity to each other. If one of the servers becomes unavailable, the remaining two will supply the licenses. If two of the three servers become unavailable, no licenses will be supplied.

After Setting Up the Licenses

After getting and setting up licenses, you are ready to start using Dimensions RM with SLM. If you have not already done so, proceed with installing Dimensions RM (see chapter "Installation Types" on page 54). Make sure that the users responsible for installing Dimensions RM know the name or IP address of the SLM server so they can successfully complete their Dimensions RM installation.

Chapter 3

Installing and Configuring Your RDBMS and Database Client

Overview

Dimensions RM can use an Oracle database or an Microsoft SQL Server database. Please find the details about these database systems in chapters "Installing and Configuring Oracle" on page 34 and "Installing and Configuring MS SQL Server" on page 45.

Installing and Configuring Oracle

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:

http://nadownloads.microfocus.com/websync/
Internap_Download.aspx?FilePath=/serena/platformmatrix/
dimensionsrm/rtm_12.7.1.xlsx

NOTE The Dimensions RM server (and all other Dimensions RM components) are 32-bit applications that can be run on either a 32-bit or 64-bit Windows platform.

- A 32-bit or 64-bit Windows Oracle Standard or Enterprise 11g2, 12, or 18 (Note *11gR1 is not supported on 32-bit Window Server 2008 or on Windows Server 2008 R2*). This can be located on either the same network node as the Dimensions RM server or a remote network node.

- A 32-bit or 64-bit UNIX Oracle Standard or Enterprise 11gR2, 12, or 18. This can only be located on a network node remote from the Dimensions RM server.

The Administrator Oracle Client

A 32-bit Oracle Administrator Client, supported by the release level of the RDBMS must be installed in a different Oracle Home in order to use the following Dimensions RM components:

- A Dimensions RM server communicating with a remote 32-bit or 64-bit Windows or 32-bit UNIX RDBMS.

- A Dimensions RM server communicating with a local 64-bit Windows RDBMS.

- A Dimensions RM Admin Client communicating with a Dimensions RM database.

- Web Server (because this uses Oracle Call Interface).

NOTE

- If you have a 32-bit Oracle installed on the same machine as Dimensions RM, you should check to see whether the 32-bit Oracle client components are installed by attempting to connect to the database using sqlplus. Install a 32-bit Administrator Oracle client if the connection test shows that it is currently absent.

- If you have a 64-bit Oracle installed on the same machine as Dimensions RM, you will need to install an additional 32-bit Administrator Oracle client.

- The release levels of the Oracle client must match that of the RDBMS.

- The 32-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).

- The Oracle 11gR1 Administrator Client is not supported on Windows Server 2008 R2 or Windows 7.

TIP Oracle provides a client only install. You do not need to do another server installation to obtain the 32-bit Oracle Administrator Client.

Configuring Oracle

If upgrading to a newer release of RM on a server previously hosting RM, you may proceed directly to .

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
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)

Oracle 32-Bit client Installation

If the Oracle Server is 64-bit or if the Oracle server is running remotely, the Oracle 32-bit client must be installed on the RM application server. Please note that the Oracle client version and patch level must be supported by the server.

> **CAUTION!** Do not install the Oracle 32 bit client into the default 32-bit programs directory (C:\Program Files (x86)). If the Oracle client is installed in that directory, Dimensions RM will *not* work.

1 Run the Oracle client install (setup.exe) as Administrator, **choosing installation type Administrator**.

2 Configure TNSnames

  a Copy TNSnames file from server to client install path
For example, from
…\Oracle_install\NETWORK\ADMIN\tnsnames.ora
To
…\32bitClient\product\11.2.0\client_1\network\admin\tnsnames.ora

  b To ensure correctness, modify the 64-bit specific alias:

   In the dbhome_1\NETWORK\ADMIN\tnsnames.ora file (as a windows administrator), edit the alias to make it specific to 64-bit Oracle.

   In the following example, the alias for RMDB02 in the database install directory is changed to RMDB02.64. This allows the RM administrator to recognize immediately that the 64bit tnsnames file has been accessed.

  c For details concerning the editing of the tnsnames file see:

   http://docs.oracle.com/cd/E11882_01/network.112/e10835/tnsnames.htm#NETRF007

   ```
   RMDB02.64 =
     (DESCRIPTION =
       (ADDRESS = (PROTOCOL = TCP)(HOST = hostname)(PORT = 1521))
       (CONNECT_DATA =
         (SERVER = DEDICATED)
         (SERVICE_NAME = RMDB)
       )
     )
   ```

  d For the client's TNSnames file and a container database, add (see next page):

```
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 40.

- 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 Restart the Oracle TNSListener service.

4 **Set the PATH environment variable such that the x32 bit client path appears first (before x64) 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`

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

Deferred Segment Creation

Oracle 11gR2 added a feature called *deferred segment creation*, which also exists in subsequent versions and is on by default. This feature results in empty tables not being listed in dba_segments. Consequently the Oracle Export utility (exp) skips empty table segments by default so that they are not exported at all, even the DLL definitions.

Oracle 11gR2: For Oracle 11g, the use of the Oracle Export utility (exp) was deprecated by Oracle, instead the Oracle Data Pump export utility (expdp) is used for all Oracle backups and the associated impdp utility for all associated database imports if you wish to use native Oracle utilities. These Data Pump utilities do not suffer from the above limitation.

Oracle 12c and higher: For Oracle 12c and subsequent versions, the table export is not affected by the deferred segment creation, so the Oracle Export utility (exp) will export all tables, even if they are empty.

Prior to Dimensions RM 11.2.2, the associated RM Manage utilities **Backup/Restore Instance Account** and **Create New Instance** were also based on the legacy Oracle `exp/imp` utilities. If you plan to backup an instance account using pre-Dimensions RM 11.2.2 on Oracle Enterprise 11gR2, therefore, the RM Manage utility **Backup/Restore Instance Account** skips empty table segments. This causes an `ORA-1950` error and a

failure to retrieve a security dump from a Dimensions RM instance table when restoring a saved Dimensions RM instance (during table import from the saved dump).

The deferred segment creation database feature is controlled by the database parameter `deferred_segment_creation`. It has a default value of `TRUE`. If you set it to `FALSE`, any newly created tables after that change will be exported including empty tables segments.

Consequently, in the above circumstances, before using legacy RM Manage **Backup Instance Account** you should set the `deferred_segment_creation` parameter to FALSE as described below:

Run the following SQL Plus commands (executed as Oracle `SYS` account):

```
show system set deferred_segment_creation;
alter system set deferred_segment_creation=false;
```

IMPORTANT! The above change of behavior will be applicable only for new accounts and new tables created in existing accounts.

If a legacy RM Manage instance backup needs to be taken of an existing Dimensions RM instance account, the following SQL Plus command must be executed to fix existing empty tables (again to be executed as Oracle SYS account):

```
declare

begin
FOR tables in (select table_name from user_tables where num_rows=0)
LOOP
EXECUTE IMMEDIATE 'ALTER TABLE ' || tables.table_name || ' ALLOCATE
    EXTENT';
END LOOP;
end;
/
```

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 43, 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 43 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**.

Installing and Configuring MS SQL Server

MS SQL Server System Requirements

Supported MS SQL Server 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:
>
> http://nadownloads.microfocus.com/websync/
> Internap_Download.aspx?FilePath=/serena/platformmatrix/
> dimensionsrm/rtm_12.7.1.xlsx

> **NOTE** The Dimensions RM server (and all other Dimensions RM components) are 32-bit applications that can be run on either a 32-bit or 64-bit Windows platform.

- Microsoft SQL Server 2016 SP1 or higher

- A database instance which will receive the data of the Dimensions RM instances to be created.

- A 32-bit System DSN which allows connection to MS SQL 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 2016 SP1 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 2016 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** and any other feature desired or required.

10   Click **Next**.

11   Ensure that the **Default instance** option is selected.

12   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**.

13   Click **Next** twice.

14   Select **Mixed Mode (SQL Server authentication and Windows authentication).**

15   Enter a password for the sa account in the **Enter password** and **Confirm password** boxes. Take a note of the password.

16   Click **Next**.

17   Click **Install**.

18   After installation is complete, verify that all setup steps have the status **Succeeded**.

19   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 **SQL Server 2016 Configuration Manager**.

2   Expand **SQL Native Client 11.0 Configuration (32bit)**.

3   Select **Client Protocols**.

4   If **Named Pipes** is enabled, right-click **Named Pipes** and select **Disable** from the shortcut menu.

5   If **TCP/IP** is disabled, right-click **TCP/IP** and select **Enable** from the shortcut menu.

6   Expand **SQL Server Network Configuration**.

7 Select **Protocols for *MSSQLSERVER***. Note that you may see a different name than *MSSQLSERVER* if you changed the instance name during setup.

8 If **Named Pipes** is enabled, right-click **Named Pipes** and select **Disable** from the shortcut menu.

9 If **TCP/IP** is disabled, right-click **TCP/IP** and select **Enable** from the shortcut menu.

10 Expand **SQL Native Client 11.0 Configuration**.

11 Select **Client Protocols**.

12 If **Named Pipes** is enabled, right-click **Named Pipes** and select **Disable** from the shortcut menu.

13 If **TCP/IP** is disabled, right-click **TCP/IP** and select **Enable** from the shortcut menu.

14 Select **SQL Server Services**.

15 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.

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 17.4 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 Shared 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 not installed on the same machine, see chapter "Installing the ODBC Driver for MS SQL Server for Separate Setups" on page 49.

To install the ODBC driver for MS SQL Server 2016 SP1, execute these steps:

1 Download the 64-bit ODBC driver for MS SQL Server.

2 Double-click `msodbcsql_64.msi`. This opens the **Microsoft ODBC Driver 11 for SQL Server 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 Click **Install**.

7 Click **Finish**.

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, see chapter .

To install the ODBC driver for MS SQL Server 2016 SP1, execute these steps:

1 Download the following parts of the Microsoft SQL Server 2016 Service Pack 1 Feature Pack (ENU refers to English download):

- ENU\x64\msodbcsql.msi

- ENU\x64\MsSqlCmdLnUtils.msi

- ENU\x64\sqlncli.msi

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\SysWOW64`.

2 Start `odbcad32.exe`.This opens the **ODBC Data Source Administrator (32-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 (32-bit)** dialog.

> **NOTE** RM Import Client does not require the ODBC data source (it communicates to Dimensions RM via Web services).

Chapter 4
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. It has been stated before, but must be stated again: This option requires Microsoft Office (32-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), otherwise RM Import will not be available for installation.

Final Checks

> **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 Serena License Manager (SLM) installed with RM Licenses, unless planning to use the 30-day evaluation.

3 32-bit 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\Micro Focus\Dimensions 12.7.1\RM`

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

One More Tomcat Reminder

IMPORTANT! All Dimensions RM releases following 12.1.x 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.

Installing on Windows Server 2012 R2 and higher

This chapter describes the steps to take before installing Dimensions RM on Windows Server 2012 R2 and higher.

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**.

10 Open **Server Manager**.

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

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

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

13 Select one of the following:

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

14 Click **Next**.

15 Click **Install**.

> **NOTE** RM Import requires Microsoft Office 2010 SP1 or higher to be installed. If you are installing Microsoft Office, also see chapter "Support for Publishing / Word Import" on page 65.

16 Restart the server.

Running Setup.exe

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

2 Accept the license agreement.
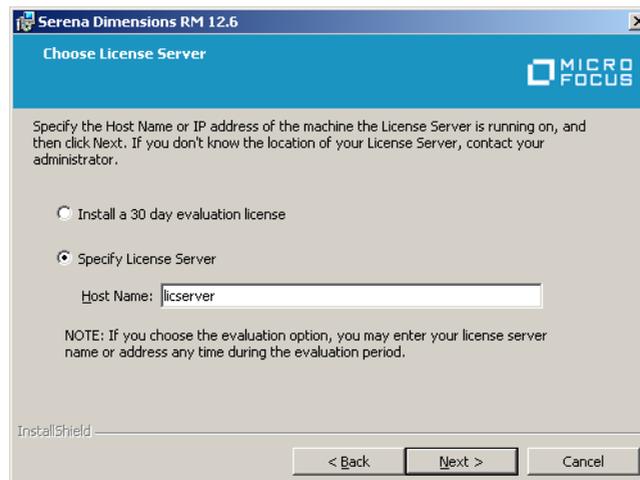
3 Select the **Server** installation.
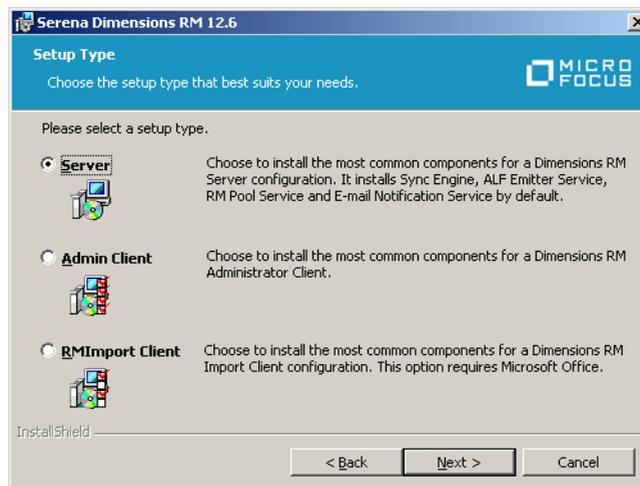
4 If desired, change the destination folder.

5 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; in the example below Single Sign On (SSO) will not be installed.

Please note that SSO requires either an SBM or Dimensions CM installation.
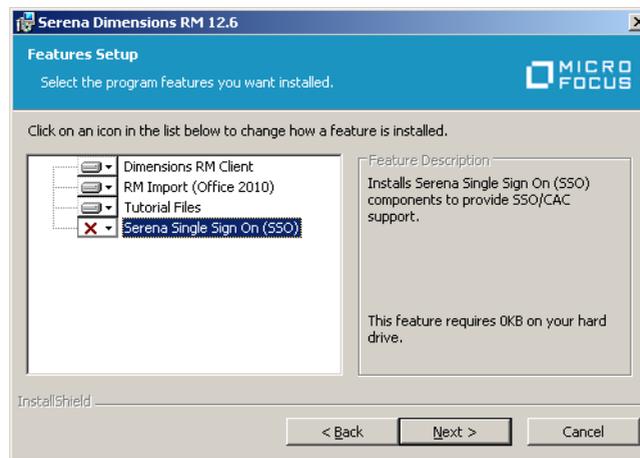
6 Select the License Server: enter the IP address or host name for the Serena License Manager (SLM) location. If the license manager has not yet been installed, choose **30 day evaluation**.


7 On the Tomcat Dialog – allow the default, **8080**, assuming ports have been checked to ensure that there is no conflict.
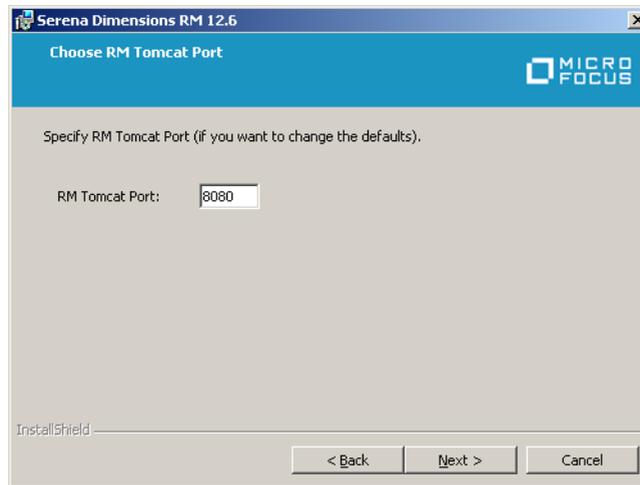
8   Select the database version. If you select **MS SQL,** you will continue with step 10.

9   Select the Oracle installation. If the list does not contain your Oracle installation, click **Manual Entry**.

   a   Enter the Oracle Home path (for RM must be the 32bit client home).

   b   Enter the Oracle SID.

10   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 (x86)\Micro Focus\Dimensions 12.7.1\RM\security.dat`

11   Check the **Add Shortcuts** box – if shortcuts are wanted – and click on **Install**.

12   Once the *Successfully Completed* install dialog is raised, click on **Finish**.
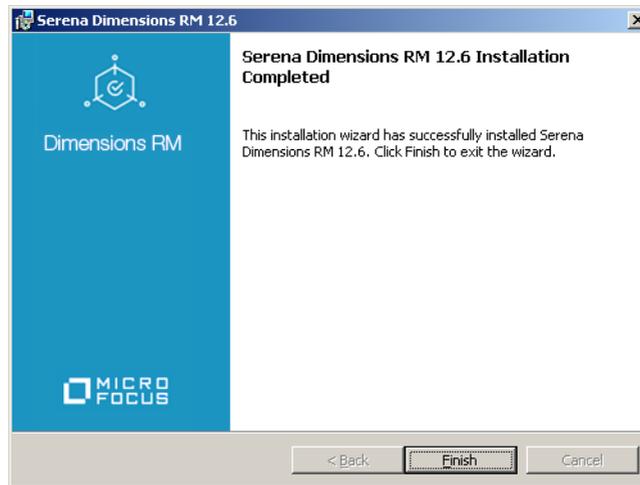
Running Setup.exe without Internet Connection

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 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**.

22 Start Setup.exe.

Chapter 5
Post-Installation Activities for a Fresh Dimensions RM Installation

Chapter Overview

This chapter discusses the post-installation procedures and checks that are required following the fresh installation of a Dimensions RM Server. For a Dimensions RM Admin Client or RMImport Client installation ceratin of these procedures will not be applicable, principally those with reference to the RM Browser and Web Servers.

For post-installation procedures and checks specifically for Dimensions RM upgrade installations, see "Post-Installation Activities for an Upgraded Dimensions RM Installation" on page 129.

🛑 **IMPORTANT!** When using RM Manage or RM Class Definition from a client machine, the changes will not take effect until the **Micro Focus Dimensions RM Pool Manager** service is restarted on the RM server.

Checklist

✓	Checklist Items
	Check that the installation has completed successfully (see "Checking That the Installation Has Completed Successfully" on page 63).
	Check that the Windows services are setup correctly and running (see "Checking Windows Services" on page 63).
	Check that the License server is running and licenses are available (see "Licensing Dimensions RM Products" on page 64).
	Set the optional security message if you have installed to a secure system (see "Setting the Optional Security Message" on page 64).
	Install or configure MS Office to allow document publishing (see "Support for Publishing / Word Import" on page 65).
	Check for updates (see "Checking for Latest Updates" on page 70).
	Set up the database schema and ICDBA Account (see "Creating the ICDBA Account" on page 71).
	Import an example Dimensions RM instance (see "Importing a Sample Dimensions RM Instance" on page 78).
	If you installed the Single Sign On (SSO) components, configure SSO (see "SSO and CAC Configuration" on page 82).
	Configure the Web Server for RM Browser (see "Configuring the Web Server for RM Browser" on page 90).
	Configure the Web Server for RM Import and RM Import Designer (see "Configuring the Web Server for RM Import and RM Import Designer" on page 90).
	If applicable, enable Dimensions CM-Dimensions RM ALM Integration (see "Prerequisites for the Dimensions CM to Dimensions RM Integration" on page 91).

	If applicable, enable an instance for ALF Events (see "ALF Enabling a Dimensions RM Instance" on page 92).
	Check if RM Browser is accessible (see "Test Browser Access" on page 90).
	Quickly check out the Dimensions RM installation (see "Quickly Checking the Installed and Configured Dimensions RM Server" on page 92).

Immediate Dimensions RM Post-Installation Activities

Checking That the 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. Select the appropriate entry (for example, **Dimensions RM 12.7.1**) and click the **Click here for support information link** to check the version number.

Checking Windows Services

1 Log in as a user with local Windows administrative rights. Access Services by:

`Start | Control Panel | Services`

or

`Start | Control Panel | Administrative Tools | Services`

This will display the status of the services for your particular Windows PC.

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

- Dimensions RM services:

  `Micro Focus Dimensions RM Pool Manager`
  `Serena License Server(*)`

  (*) This service may be absent if you are using Serena License Manager (SLM) on another server. If the service should be present and is not running, refer to "Starting the License Server" on page 28 for instructions on setting it up.

- **Oracle only:** Oracle services

  `OracleDBConsoleRM`
  `Oracle<oracle_service_name>TNSListener(*)`
  `OracleService<oracle_service>(**)`

  (*) By default this will be `OracleDimensionsTNSListener`.

  (**) See chapter "The Database Instance Creation Details" on page 36.

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

- Dimensions RM processes (note that there will be several rmAppServer.exe
  processes for a default installation):

  rmAppServer.exe
  RMServerPool.exe

- When using Oracle only: Oracle Enterprise only processes:

  oracle.exe
  TNSLSNR.EXE

Licensing Dimensions RM Products

See "Licensing Dimensions RM" on page 23 details about licensing Dimensions RM
components.

Setting the Optional Security Message

If you are installing to a secure system, you must enable the optional security warning as
soon as installation is complete. Please see the topic "Creating Custom Login Alert Pages
for RM Browser" in the *RM Administrator's Guide*.

Virus Checkers

Real-time virus checking of certain Dimensions RM and Oracle database files can cause a
noticeable slowdown in 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 *(continued on next page)*	■ Run as system user continuously once the product is installed. ■ Memory usage of this particular process increases/decreases depending upon the load.	This executable is continuously using the active system memory and is accessed by each and every request over the Internet or intranet.
Datacacheserver.exe *(continued)*	■ Multiple process are launched and run in the memory.	

File Name	Execution Mode	Risks Introduced by Excluded from Real-Time Virus Checking
Oracle.exe	▪ Run as system user continuously once the Oracle is installed and the instance is started. ▪ Memory usage of this particular process increases/decreases depending upon the load.	As above.
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.
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.

Support for Publishing / Word Import

In order to allow publishing and importing documents, Dimensions RM needs to access Microsoft Office (32-bit). As the standard configuration of Windows Server does not allow this, the Windows Server installation needs to be modified as described in the following chapters.

To allow the SYSTEM user account to access Microsoft Office, create these folders:

▪ `C:\Windows\System32\config\systemprofile\Desktop`

▪ `C:\Windows\SysWOW64\config\systemprofile\Desktop`

Publishing on Windows Server 2012 R2

To allow the SYSTEM user account to access Microsoft Office, create these folders:

- `C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Windo ws\INetCache`

- `C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windo ws\INetCache`

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, click **Change account type**. In Icon view click **User Accounts**. Then click **Manage User Accounts**.

3 Select the **Advanced** tab.

4 In the **Advanced user managment group**, click **Advanced**. This opens the **Local Users and Groups** dialog.

5 In the **Local Users and Groups** dialog, right-click the folder **Users** and select **New User...** from the shortcut menu. This opens the **New User** dialog.

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

7 In the **password box**, enter a complex password.

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

9 Take a note of that password.

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

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

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

13 Click **Create**.

14 Click **Close**.

15 Select the **Administrator** option.

16 Click **Finish**.

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

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

19 Select the **Member Of** tab.

20   Click **Add...**

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

22   Click **OK**.

23   Click **OK**.

24   Change to the log on page and log on with user *RmPublish*.

25   Start all installed Microsoft Office applications and confirm any dialogs.

26   Log off user *RmPublish*.

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

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

7   Click **OK**.

8   Click **OK**.

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

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

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

12   Click **OK**.

13   Click **OK**.

Using Microsoft Office on Windows Server

To allow Dimensions RM to use Microsoft Office (32-bit), the following steps have to be executed:

1   Open the Command Prompt.

2 Type services.msc and press **Enter**.

3 From the list, select the **Micro Focus Dimensions RM Pool Manager** service and click **Stop**.

4 Double-click the **Micro Focus Dimensions RM Pool Manager** service.

5 Select the **Log On** tab.

6 Select the **This account** option.

7 Enter use name and password. For the user name, use the user you created in chapter .

8 Click **OK**.

9 From the list, select the **Micro Focus Dimensions RM Pool Manager** service and click **Start**.

10 In the command prompt, type comexp.msc /32 and press **Enter**.

11 Navigate to Component Services | Computers | My Computer | DCOM Config

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

13 Select the **Identity** tab.

14 Select **The launching user.**

15 Click **OK**.

16 Ensure that you prepared the server as described earlier.

Using Adobe Reader on Windows Server

If Adobe Reader is installed on the server, publishing documents can cause RM Browser to hang. This occurs if the document you publish 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 the 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**.

Configuration and the First Instance

The newly created RM database requires configuration before it can be accessed; 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.

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

            Start | All programs | Micro Focus | Dimensions RM 12.7.1 | 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 – please check the box and set the ICPROJECTS account with the same process, as shown below. These are NOT login accounts.

> **NOTE**   The passwords for ICADMIN and ICPROJECTS must be UPPER CASE. It is our best practice recommendation to make the ICADMIN and ICPROJECTS passwords the same.

d   The next step is to name the instance, RMDEMO, and to set the RMDEMO instance administrator account password - as shown below. 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.

Checking for Latest Updates

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

<http://supportline.microfocus.com>

to determine the latest patch updates for Dimensions RM, if any. This site requires first time users to register for a user name and password.

Once logged into the support site, under `Support | My Downloads` you will find an option to download patches (select **Dimensions RM** from the **Please Select Product** dropdown list and then click the **Click here for Patches** link next to the dropdown list). Search the list of patches to see if there are any maintenance patches appropriate to your version of Dimensions RM. If there are any such patches, it is normally recommended that you download them together with the associated patch readme and apply them. Each

patch download normally includes the patch binary, an integral patch installer, and the associated patch readme that includes instructions for running the patch installer.

Creating 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)

    Starting with Dimensions RM 11.2.1, you now have the option of creating the ICDBA database account (and associated password) from within RM Manage.

    See "Creating the ICDBA Account From Within RM Manage" on page 71.

- **Oracle only:** Using the "setupRM.sql" Script (or your own edited version)

    You or your database administrator (DBA), as an Oracle SYSDBA user (for example, SYS), can manually run the pre-prepared setupRM.sql SQL script located at:

    <install directory>\Micro Focus\Dimensions *<version>*\RM\sql

    for example:

    C:\Program Files\Micro Focus\Dimensions 12.7.1\RM\sql\
        setupRM.sql

> **IMPORTANT!** If you run an edited version of the script, it should be noted that Dimensions RM requires the user account ICDBA to be upper case and the associated password is case sensitive.

The procedure for running this script is described in "Running the setupRM.sql SQL Script" on page 72. See also, "Changing the ICDBA Password in the setupRM.sql SQL Script" on page 73 and "Sample SQL Scripts for Oracle Databases" on page 76.

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 (for example, RM).

2   Select **File | Create ICDBA Account**, click the **Create ICDBA Account** button 🖳, or right-click the database and select **Create ICDBA Account**.

3   The **Create ICDBA account** dialog box opens.

4   In the **Password** field of the **Create ICDBA account area**, type the password that you want to assign to the Dimensions RM ICDBA account.

> **IMPORTANT!** The password must be in upper case only.

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

6   In the **Account Name** field of the **Enter SYSDBA account password** area, enter the appropriate SYSDBA account that you want to use. For Oracle, it is usually SYS; for MS SQL Server it is usually sa.

7   In the associated **Password** field, type the associated password for the account name.

8   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.

9   Click **Create**.

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 using the RM Manage **Change Administrator Password** menu item, see "Changing Database Administrator Account Passwords Using RM Manage" on page 76.

Running the setupRM.sql SQL Script

Follow these steps to configure the schema and create the ICDBA account:

1   Open a Windows Command Prompt window:

    All Programs | Accessories | Command Prompt

2   Navigate to the location of the setupRM.sql file, for example:

    C:\Program Files\Micro Focus\Dimensions 12.7.1\RM\sql\
        setupRM.sql

3   In the Command Prompt window, enter the following commands:

    sqlplus sys/<password>@<databasename> as sysdba
    SQL> @setupRM.sql
    SQL> exit

for example:

    sqlplus sys/change_on_install@rm as sysdba
    SQL> @setupRM.sql

```
SQL> exit
```

> **NOTE** The error message:
>
> ```
> ORA-01543: tablespace 'USERS' already exists
> ```
>
> can be safely ignored.

Changing the ICDBA Password in the setupRM.sql SQL Script

You may wish to change the ICDBA password to something other than the default `ICDBA` in the `setupRM.sql` file (it must be in upper case) before running it.

To change the ICDBA password:

1 Open the `setupRM.sql` file in a text editor.

2 Locate the following line:

```
create user ICDBA identified by ICDBA default tablespace users;
```

3 Change the second occurrence of `ICDBA` to an upper case password of your own choice. The first character must be an alphabetic character, and underscores (_) are reserved for special characters. This password is not case-sensitive. The following example line includes the password `RM_123`:

```
create user ICDBA identified by RM_123 default tablespace users;
```

4 Save the file.

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>*\Micro Focus\Dimensions *<version>*\RM\ on a regular basis.

Starting with Dimensions RM 11.2.1, you can change the passwords for the Dimensions RM database administrator Oracle accounts ICDBA, ICADMIN, and ICPROJECTS from within RM Manage —see .

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 11 the new 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
    ICPROJECTS
    <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 and ICPROJECTS accounts 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;
ALTER USER ICPROJECTS 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

Starting with Dimensions RM 11.2.1, for the Dimensions RM database administrator accounts ICDBA, ICADMIN, and ICPROJECTS you now have the option of changing their passwords from within RM Manage.

To change the ICDBA, ICADMIN, or ICPROJECTS account password:

1 Select the database whose administrator accounts (one or more of ICDBA, ICADMIN, or ICPRPOJECTS) 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, ICADMIN, or ICPROJECTS account 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.

Sample SQL Scripts for Oracle Databases

Dimensions RM installs various sample scripts in the directory:

```
<install directory>\Micro Focus\Dimensions <version>\RM\sql
```

for example:

```
C:\Program Files\Micro Focus\Dimensions 12.7.1\RM\sql\
    setupRM.sql
```

These are primarily intended for knowledgable DBAs and comprise the following:

setupRM.sql

See "Creating the ICDBA Account" on page 71.

SetupDatabase.bat

A Windows batch file that runs the `setupRM.sql` SQL file. If used, this should be edited for your own particular set up.

icadmin-upgrade-RM2009R1.sql

A SQL file that can be used for database upgrade operations with respect to upgrading Dimensions RM 2009 R1 databases to 2010 R1. Please consult Micro Focus support for details.

icadmin-upgrade-RM2009R1.bat

A Windows batch file that runs the icadmin-upgrade-RM2009R1.sql SQL file. If used, this should be edited for your own particular set up.

icadmin-upgrade-RM2009R1SP1.sql

A SQL file that can be used for database upgrade operations with respect to upgrading Dimensions RM 2009 R1SP1 databases to 2010 R1. Please consult Micro Focus support for details.

icadmin-upgrade-RM2009R1SP1.bat

A Windows batch file that runs the icadmin-upgrade-RM2009R1SP1.sql SQL file. If used, this should be edited for your own particular set up.

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.

Importing a Sample Dimensions RM Instance

After you install Dimensions RM, you must create an instance from a provided sample instance or an existing instance backup (but see "Special Considerations When Restoring Existing Instances With E-mail Rules" on page 81). The following steps explain how to create an instance from a provided sample instance. This is just an example; you can use these steps with other instances.

> **NOTE** There are other options available for importing and creating instances, such as importing a saved instance or creating a blank instance. For information about these options, see the *Dimensions RM Administrator's Guide*.
>
> Do NOT use the QLARIUS or RMDEMO sample instances 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 the BLANK instance and then saved (see the Saved Instances tab).

To import an sample instance:

1 Start RM Manage.

2 Right click the Dimensions RM database (for example, RM) in the tree structure and select **New Instance**. The **Please enter password** dialog box opens.

3 In the **Password** field, type the password for the Dimensions RM ICDBA account.

> **NOTE** Step 4 only occurs when creating the first instance in a chosen database. For subsequent instances created in that database, you go directly to Step 5.

4 Starting in Dimensions RM 11.2.1, the passwords for database user accounts ICDBA, ICADMIN, and ICPROJECTS are no longer hard coded. The password for the ICDBA account has to be assigned first when creating that account (as explained in "Creating the ICDBA Account" on page 71); whereas, the passwords for the ICADMIN and ICPROJECTS accounts have to be assigned on first-instance creation within a database as explained here.

> **IMPORTANT!** You must ensure that you create the ICDBA account and associated password before assigning passwords to ICADMIN and ICPROJECTS. There is no software check to ensure that this has been done in the correct order.

    a The **Enter ICADMIN/ICPROJECTS password** dialog box opens.

    b In the **ICADMIN Password** field, type the password to be assigned that account.

> **IMPORTANT!** The password must be in upper case only.

    c Micro Focus recommends that you use the same password for the ICADMIN and ICPROJECTS accounts. This is done by default.

       However, if you want to assign a different password to ICPROJECTS, select the **Change ICPROJECTS password** checkbox and enter an appropriate upper case password in the **ICPROJECTS Password** field.

    d By default, the account is created in a SERENA_RM_ADMIN tablespace. To create the account in an existing tablespace, click the **Advanced** button. The dialog expands to display the advanced features:

       • To create the 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.

    e Click **OK**.

> **IMPORTANT!**
>
> ■ When creating the accounts for ICADMIN and ICPROJECTS, Dimensions RM automatically generates a new `security.dat` file. The old version of this file is renamed and retained as a backup.
>
> ■ 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 ICADMIN and ICPROJECTS passwords before 180 days elapse using the RM Manage **Change Administrator Password** menu item, see "Changing Database Administrator Account Passwords Using RM Manage" on page 76.

5 The **Please Enter Instance Information** dialog box opens.

6   Type an instance name in the **Instance Name** field (for example, MYINSTANCE).

7   Type an instance password in the **Instance Password** field (for example, MYINSTANCE) and retype it in the **Confirm Instance Password** field.

8   Type a system administrator password in the **Administrator Password** field (for example, MYINSTANCE). (An Oracle privileged account is required to create new instances.)

9   Retype the system administrator's password in the **Confirm Administrator Password** field, and click **OK**. The new instance will now be created.

> **NOTE** The instance password is one that Dimensions RM uses as a database user password. It is not needed to use Dimensions RM. The administrator account (which is automatically created and named by appending ADMIN to the instance name, for example, MYINSTANCEADMIN) and password (for example, MYINSTANCE) are the ones you need to remember when you first open the instance you are in the process of creating (for example, MYINSTANCE).
>
> Starting with Dimensions RM 11.2.1, the instance administrator database account only has access rights with respect to the RM Manage tool itself. No other Dimensions RM tools can be accessed with this account.

Depending on the sizes of various tables in your database, for particular tables, **Tablespace Error** dialog boxes may open during instance creation to indicate that a particular table is not at high enough value. If this occurs, for each **Tablespace Error** dialog box:

a   Read and take note of the error message in the dialog box.

b   Click **Yes**. A **Resize Tablespace** dialog box will open.

c   In the **Resize Tablespace** dialog box, enter in **New Datafile Size** the new tablespace size increased (at least) as recommended in Step a.

d   Click **Resize**. A **Resize** dialog box will open.

e   In the **Resize** dialog box, click **Yes**.

f   In the **Resize Tablespace** dialog box, click **Close**.

10   Click **OK** in the **Success** dialog that informs you that the instance has been created. The **Import** dialog opens.

11   Click the Sample Instances tab and select a sample instance (for example, RMDEMO).

> **IMPORTANT!** Do NOT use the QLARIUS or RMDEMO sample instances 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 the BLANK instance and then saved (see the Saved Instances tab).

12   Select the **Include Security Data** check box. This will enable you to include user accounts, user groups, and access right definitions in the sample instance.

13   For sample instances such as RMDEMO, a buffer of 1 MB is sufficient, so you can accept the default value in the **Buffer Size (Mb)** list.

14 Click **Install**. After the installation is complete, you are prompted whether you want to view the log file. Click **Yes** or **No** as appropriate.

> **NOTE** See the Dimensions RM readme for information on possible database errors that can be safely ignored.

15 Exit RM Manage.

Your new instance (for example, MYINSTANCE) based on a sample instance (for example, RMDEMO) will now be available for use. You can test its availability as follows:

1 Start RM Manage.

2 Click the Dimensions RM database (for example, RM) in the tree structure. The **Logon Information** dialog box opens.

3 In the **User Name** field, type the name of the system administrator for the instance that you just created (for example, MYINSTANCEADMIN).

4 In the **Password** field, type the password of the system administrator for the instance that you just created (for example, MYINSTANCE).

5 Click **OK**.

6 In the **RM Manage** dialog box, click the '+' sign next to the Dimensions RM database (for example, RM) in the tree structure. Your new instance (for example, MYINSTANCE) will appear in the tree structure and will be labeled (current).

   If the instance is not shown as (current) it will need to be converted as follows:

   a Select the database that contains the instance you want to convert.

   b Select **File | Convert Database**, click the **Convert Database** button 🖧 , or right-click the database and select **Convert Database**. This starts the conversion tool.

   c To expand the database that contains the instance you want to convert, click + next to the database name.

   d Enter the ICDBA password.

   e Select the instance and click **Upgrade**.

   f To start the upgrade, click **Continue**. The upgrade may take several minutes to complete.

> **NOTE** For more information about working with instances, including creating Dimensions RM users, see the *Dimensions RM Administrator's Guide*.

Special Considerations When Restoring Existing Instances With E-mail Rules

If you create a new instance from the back up of an existing instance, there are special considerations that need to be taken into account if the existing instance uses e-mail rules.

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.

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. The Micro Focus SSO server is an optional part of a Dimensions CM or SBM installation.

For information about installing and configuring the Micro Focus SSO server, see the Dimensions CM or SBM documentation.

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.

See "Exporting a Certificate from IIS" on page 82, "Exporting a Certificate from the STS Server" on page 83 and "Adding a Certificate for RM Server to the STS Keystore" on page 83.

- 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 of Dimensions RM 12.1, Dimensions RM includes its own Tomcat web server, so Apache and IIS are not required, though you can optionally run a third-party web server in addition to the Micro Focus Common Tomcat web server if you wish to avail yourself of the security and management features of a third-party web server.

1   Retrieve the certificate in CER format by following the steps in chapter "Exporting Certificates to CER Format from IIS" on page 137.

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/

Exporting a Certificate from the STS Server

After you have configured the Dimensions CM or SBM STS server with your own SSL certificates (rather than the demo certificates it may have shipped with), 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 141 or "Exporting the STS Certificate from SBM Configurator" on page 142.

> **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 (x86)\Micro Focus\Dimensions 12.7.1*\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 86.

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 136 or "Exporting Certificates to CER Format from IIS" on page 137.

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 (x86)\Micro Focus\Dimensions 12.7.1*.
>
> ■   Replace **#.#.#.#** with the Common Tools version number, e.g. *1.8.3.0*.
>
> ■   Replace **#.#** with the Java version number, e.g. 8.0.
>
> The complete set command may look like this:
>
> `set path=%path%;"`*`C:\Program Files (x86)\Micro Focus\Dimensions`*` 12.7`
> `.1\Common Tools `*`1.8.3.0`*`\jre\`*`8.0`*`\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 them. The SSO login source is enabled via the RM Manage interface. See the *Dimensions RM Administrator's Guide* for details.

Registry Keys and Configuration Files on the RM Server

The following sections list 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\Wow6432Node\Serena Software\RTM\Environment
\Default
```

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 (x86)\Micro Focus\Dimensions 12.7.1\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 (x86)\Micro Focus\Dimensions 12.7.1\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 (x86)\Micro Focus\Dimensions 12.7.1\RM\conf\sts.pem`
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 Micro Focus 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 Micro Focus 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.

gatekeeper-services-config.xml	
Parameter	**Description**
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"/>	

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\Wow6432Node\Serena Software\RTM\Environment
\Default
```

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 (x86)\Micro Focus\Dimensions 12.7.1`
	    `\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 (x86)\Micro Focus\Dimensions 12.7.1`
	    `\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

If SSO connections fail, this may be due to the following:

1   **Certificate sts.pem mismatch**
    Update the certificate as described in chapter .

2 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.

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.

Configuring the Web Server for RM Import and RM Import Designer

The Dimensions RM installer configures the Web server for RM Import and RM Import Designer; no manual configuration is required. For reference, the following sections summarize the tasks the installer performs to configure the Web server.

Access to Windows System TEMP Directory

See

Test Browser Access

Using the hostname or ip address, the port selected for RM Tomcat (default 8080), run rtmBrowser. On the RM server, the URL might be
`http://localhost:8080/rtmBrowser/`

For first installations, only the administrator account created during installation will exist, and only the RMDEMO instance will be selectable.
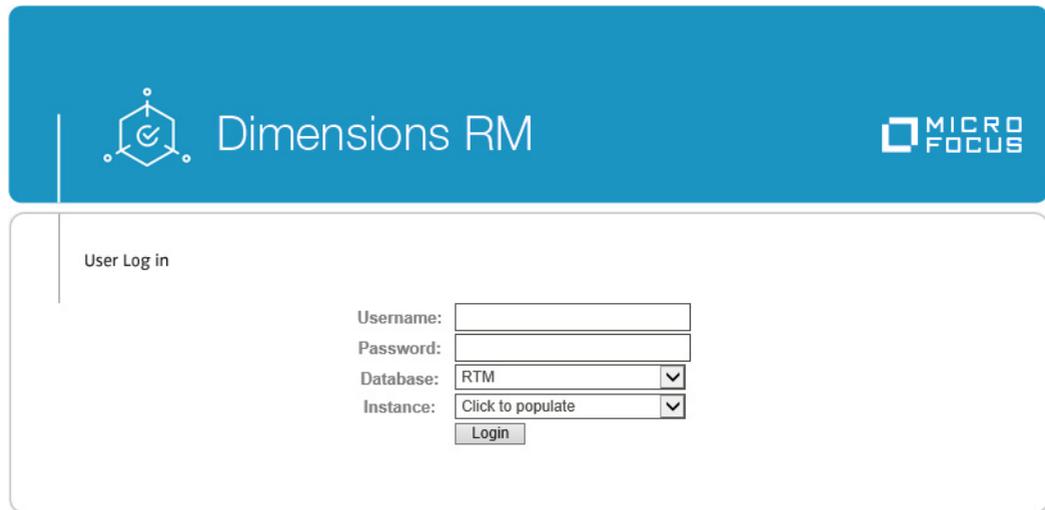
Once you are sure that the passwords are functioning, and the browser can be accessed, step through chapter .

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

Prerequisites for the Dimensions CM to Dimensions RM Integration

To set up ALM the associations, 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: http://nadownloads.microfocus.com/websync/ Internap_Download.aspx?FilePath=/serena/platformmatrix/ dimensionsrm/rtm_12.7.1.xlsx.

- A Dimensions CM desktop client must be installed on the Dimensions RM web server machine.

- For certain installations (as described in this guide), it is recommended that Dimensions RM databases have exclusive use of their own Oracle instance. In those circumstances, if you are using Dimensions CM against an Oracle RDBMS, you must make sure that it does not share the same Oracle instance as that used by Dimensions RM.

- Before you can begin to establish any of the Dimensions RM to Dimensions CM associations referred to below, the rmcm.xml configuration file on the Dimensions RM web server machine must first be edited to include the URL of the Dimensions CM server. Proceed as follows:

  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 has 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 administrator:

• 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.

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.

Quickly Checking the Installed and Configured Dimensions RM Server

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

1 If you have not already imported an RMDEMO sample instance into a new instance MYINSTANCE, please proceed to "Importing a Sample Dimensions RM Instance" on page 78. Ensure that you select the **Include Security Data** check box described in Step 12 on page 80, this will enable you to include user accounts, user groups, and access right definitions in the sample instance.

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

MYINSTANCEADMIN

■ Password

MYINSTANCE

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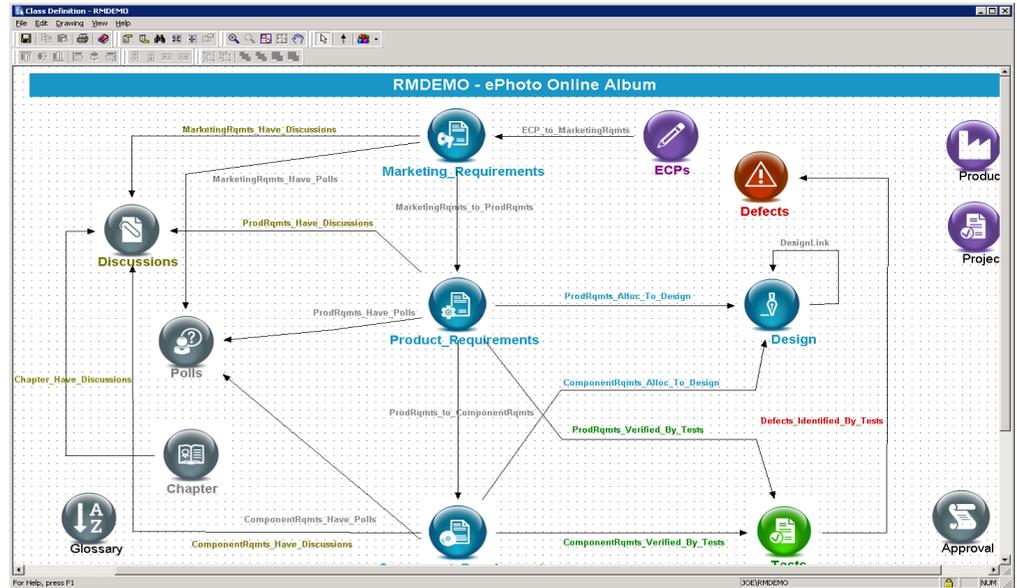
    g Save the class definition and exit the **Class Definition** tool:

```
File | Save

File | Exit
```

    h Log out of RM Manage.

4 In RM Browser, publish a traceability report for EPHOTO:

    a Log in using the following parameters:

        ■ Username

            Ephoto

        ■ Password

            RTM

        ■ Database

            <database_name> (for example, RM)

        ■ Instance

            <instance_name> (for example, MYINSTANCE)

    b Click the Requirements tab.

    c Click the Reports sub-tab.

    d In the left hand navigation tree, double click **Traceability Reports**.

    e Click **ePhoto Marketing Requirements Trace**.

    f Click the Documents tab.

    g Click the All Documents sub-tab.

    h Double click **ePhoto Requirements**.

    i Click the **Addition toolbar buttons** toolbar button

> **j**   Click the **Publish** toolbar button

> **k**   Save the generated Word document.

> **l**   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, publish a traceability report for the new user TEST99:

    a Log in using the following parameters:

        ■ Username

            test99

        ■ Password

            test99

        ■ Database

            <database_name> (for example, RM)

        ■ Instance

            <instance_name> (for example, MYINSTANCE)

    b Repeat the through to .

9 In RM Browser, create a requirement for the logged in user TEST99:

    a Click the Requirements tab.

    b Click the **New** toolbar button   The **New** dialog box appears.

    c Select **Component_Requirements** from the **Class** drop down list and ensure that the **Category** drop down list is pre-populated with your demo instance MYINSTANCE.

    d Populate the **Title** and **Text** text fields with suitable entries.

    e Check **Close requirements after save**.

    f Click **Save**.

    g Click the Categories sub-tab if it is not already selected.

    h The new requirement will be located at the bottom of the list of requirements in the **Component_Requirements** list.

    i Log out of RM Browser.

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

Enabling My Work Page

The My Work page is deprecated and will be removed in a future version of Dimensions RM. Thus it has been disabled and all views have been moved to the Dashboard. If you want to use it, you can enable by executing the following steps:

1 Stop the **Micro Focus Common Tomcat** service.

2 In Windows Explorer, navigate to
`RM_Install\Common Tools x.x\tomcat\x.x\webapps\rtmBrowser\rm\frame\panels\top`.

3 Open the file toppanel.jsp with a text editor, e.g. Notepad.

4 Search for **<%-- MYWORK --%>**.

5 Enable the following code block by removing **<%--** and **--%>**. The result should look like this:

```
<%-- MYWORK --%>
<sct:largeButtonItem href="javascript:SERENA.rm.panels.top.navigateToMyWork()">
    <span class="glyphicon glyphicon-briefcase">&#xe139;</span>
    <fmt:message key="RM_TopPanel_MyWork" bundle="${RM_TopPanel}" />
</sct:largeButtonItem>
```

6 Save the file.

7 In Windows Explorer, navigate to
`RM_Install\Common Tools x.x\tomcat\x.x\work`.

8 Delete all content in the directory.

9 Start the **Micro Focus Common Tomcat** service.

Chapter 6

Upgrading an Earlier Release of Dimensions RM

Upgrade Scenarios and Their Execution

For new installations see chapter "Installing Dimensions RM" on page 53.

There is, strictly speaking, no "upgrade" mechanism for Dimensions RM; the older version must be un-installed before initiating the installation of the 12.7.1 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, with references, are listed below.

   a Perform all pre-upgrade tasks, including backing up the database, all Dimensions RM instances, and un-installing RM. Please refer to chapter "Pre-Upgrade Tasks" on page 101.

   b Dimensions RM release 12.7.1 requires the Serena License Manager (SLM) release 2.3.0. If not already running SLM 2.3.0, upgrade the SLM. Please refer to chapter "Upgrade the Serena License Manager" on page 104.

   c Install the new release of Dimensions RM. Please refer to "Running Setup.exe" on page 56. (Do NOT continue with subsequent sections in Chapter 4).

   d Copy the security.dat file from the backed-up RM folder into the installation folder under RM. There will exist in that location the security.dat file created as part of the setup - that file can be over-written.

   e Convert / Upgrade all RM Instances. Please refer to "Create and Restore Instances in New Database" on page 106.)

   f Place saved or backed-up files in their proper locations, see chapter "Restoring Certain Dimensions RM Files" on page 107.

> **CAUTION!** During same-server upgrades you must not change:
>
> - Server names.
> - Instance names.
> - Database names.
>
> If you wish to do any of these, contact Micro Focus Support.

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. Please refer to chapter "Pre-Upgrade Tasks" on page 101.

   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 if that is not done as part of Chapter 3.
   - 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 32bit client, if not included with the Oracle install. Please refer to chapter "Configuring Oracle" on page 35.

d Install the new release of Dimensions RM. Please refer to "Installing Dimensions RM" on page 53.

e Place saved or backed-up files in their proper locations, see chapter "Restoring Certain Dimensions RM Files" on page 107.

f Restore all RM Instances. Please refer to "Create and Restore Instances in New Database" on page 106.

> **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.

Pre-Upgrade Tasks

This section details the tasks that must be undertaken prior to initiating the upgrade.

Record the Dimensions RM Mail Configuration

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

2 Record the RM Mail configuration:

a Select:
```
(Windows) Start | Micro Focus | 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. This requires that no users are accessing Dimensions RM while instance data is secured. To ensure this, stop these services:

- Micro Focus Common Tomcat

- Micro Focus Dimensions RM Pool Manager

- Micro Focus Dimensions RM E-Mail Notification Service

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

1   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.

a   If migrating to a new RDBMS - please make a note of the instance / tablespace names as well as the size of each instance's tablespace.

- At **import time**, you will be prompted to enter the *From User* as well as the *Tablespace Name*. The *From User* refers to the instance name. 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 a tablespace for 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. This will list the current tablespace names. You might also check with your DBA.

- Select **Administer Tablespaces**, and check the size of each instance tablespace. If the instance is – and will remain – active, double the tablespace to be assigned when the new instance is created.

2   Using RM Manage, right click on the instance, and select **Backup/Restore Instance Account**

Backup/Restore Instance Dialog	
Field	**Description**
Legacy/Compatibility Mode	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 Directory Path	This field is automatically populated with the default backup path on the Oracle server.

Backup/Restore Instance Dialog	
Field	**Description**
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. **NOTE** In normal mode, the location is relative to the Oracle directory path. In Legacy Mode, the path to the Saved Projects directory of the RM installation is prepended to the file name. **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_20141029_0946FinalForUpgrade.dmp
Security Data	Exports all the users that have been assigned to this instance, as well as their permissions, so that they may be imported into another database or instance.
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.

3 Rename the backup file such that it can be easily differentiated from standard instance backups, e.g., RMDEMO_20141029_0946FinalForUpgrade.dmp.

4 Click the **Backup** button. The backup operation runs.

> **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

5 Repeat the preceding steps for each instance.

6 Because the uninstall and re-install will overwrite necessary files, please copy the following files to a temporary but safe place:

a Copy the RM directory tree to a backup. For example (all in one line):
```
copy "C:\Program Files (x86)\Micro Focus\Dimensions 12.6\RM"
C:\RM12.6_Backup
```

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

```
copy
"C:\Program Files (x86)\Micro Focus\Dimensions 12.6\Common Tools
1.8.0.0\tomcat"
```

```
C:\RM12.6_tomcatBackup
```

7 If there are modified instances in the RM\Saved Projects directory, they too should be backed up.

8 **Stop all RM related Services**:

    a Micro Focus ALF Event Emitter

    b Micro Focus Common Tomcat

    c Micro Focus Dimensions RM E-Mail Notification

    d Micro Focus Dimensions RM Pool Manager

    e Micro Focus SyncEngine

9 Stop RM related Processes

    rmLicenseAgent.exe

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

11 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.

> **CAUTION!**
>
> **Jscript:** Do **NOT** restore 11.x `rtmBrowser\jscript` or `rtmBrowser\jscripts` files to a 12.1.0, or newer, installation. The files are **NOT** compatible. If customized, you must manually edit the new files to re-implement the customizations that you wish to retain.

> **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.

Upgrade the Serena License Manager

> **NOTE** For additional details concerning the license manager installation see chapter "Licensing Dimensions RM" on page 23.

Dimensions RM 12.7.1 requires SLM Version 2.3.0. To upgrade from any previous version of the *Serena License Manager* (SLM) to this required version, please proceed as follows:

1 Shut down your existing version of SLM.

2 Back up the following files in the existing SLM installation directory:

    ■ Windows

        • `merant.opt` (if you created such a file)

        • `serena.lic`

    ■ UNIX

        • `licmgr.ini`

        • `merant.opt` (if you created such a file)

- `serena.lic`

- `users.lst`

3 Uninstall the existing SLM.

4 Install the new version of SLM, see the *Installing the Serena License Manager* guide.

5 Restore the files in Step 2 to the new SLM installation directory and start SLM.

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 (x86)\Micro Focus\Dimensions 12.7.1\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:
>
> - Micro Focus Common Tomcat
>
> - Micro Focus Dimensions RM Pool Manager
>
> - Micro Focus Dimensions RM E-Mail Notification Service
>
> Note that stopping Micro Focus Common Tomcat will also disable other applications using this service.

Database Conversion with RM Manage

1 If desktop icons were installed, right-click on RM Manage, otherwise from
`Start | All programs | Micro Focus | Dimensions RM 12.7.1 | RM Manage`.
Right-click and select **Run as administrator** from the context menu.

2 Highlight a relevant database name, and a prompt for the administrator user name and password will be raised. If, instead, a *Logon failure* message is displayed – then likely the `security.dat` file is incorrect.

Check to be sure that the correct `security.dat` file has been moved from the previous installation directory to the folder indicated for its storage during the install.

Dimensions RM is installed in a new folder; the security.dat file from the previous installation will remain in the previous installation folder.

3 Right-click on the database and select **Convert Database** from the download.

4 Highlight the database in the validation dialog and click on **Upgrade**.

    a You will be promoted for the ICDBA password.

    b If prompted to recreate procedures, select **Yes**.

5 Click on the **+ sign** to expand the instance list.

    a Highlight the first instance on the list, click on **Upgrade** .

    b When the *Conversion Progress* dialog is raised, click on the **Continue** button. Please note that for large instances, a *Not Responding* warning may be displayed on the dialog – please ignore and be patient.

    c Once the Summary – Upgraded message appears, close the dialog. The upgraded instance will be marked as current.

    d Continue with the next instance on the list (it is possible to select a group) until all instances have been upgraded. They will all be listed as current.

    e Close the database validation dialog.

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 102.

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.

19   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 106 and repeating the steps until all instances have been created and populated.

Post-Installation Activities for an Upgraded Dimensions RM Installation

This section details the post-installation tasks for an upgraded installation. Normally, these are the only post-installation activities that are required, that is, you do not normally need to perform those tasks required for a fresh installation as documented in chapter "Post-Installation Activities for a Fresh Dimensions RM Installation" on page 61.

CAUTION! Please ensure that you read and implement, where appropriate, the tasks documented in this section. Failure to do this may result in the installation failing (and you not being able to re-instate your existing Dimensions RM installation).

SSO Configuration

If you installed the RM Single Sign On (SSO) components, see chapter "SSO and CAC Configuration" on page 82.

Restoring Certain Dimensions RM Files

In "Back up Database, Instances, and Necessary Files" on page 102 you were advised to back up certain files. You can now restore your backed up versions of Saved Projects to the new Dimensions RM 12.7.1 installation directory.

Restoring Tomcat Files

During the setup process, a new Tomcat has been installed. This requires to carry over any modification made to the previous Tomcat installation, e.g. templates. To avoid overwriting, the Common Tools folder has been renamed bearing the extension `.backup`. If the folder originally had the name `Common Tools 1.5.2.0` it is renamed to `Common Tools 1.5.2.0.backup`. Please note that the `rtmBrowser` directory within Tomcat's webapps directory has been renamed to rtmBrowser.bak. Using the directory name from above, an installation path might be: `C:\Dimensions RM\Common Tools 1.5.2.0.backup\tomcat\6.0\webapps\rtmBrowser.bak`.

> **CAUTION!**
>
> **Jscript:** Do **NOT** restore 11.x `rtmBrowser\jscript` or `rtmBrowser\jscripts` files to a 12.1.0, or newer, installation. The files are **NOT** compatible. If customized, you must manually edit the new files to re-implement the customizations that you wish to retain.

If upgrading from RM 12.1.x, the forms and jscript folders will be located under Common Tools, for example: `C:\Program Files (x86)\Serena\Dimensions 12.1.0\Common Tools 1.5.2.0\tomcat\6.0\webapps\rtmBrowser\jscript`

> **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.

RM 11.x	RM 12.1-12.7.1
RM_Install\RM\conf	*RM_Install*\RM\conf
RM_Install\RM\rtmBrowser \forms	*RM_Install*\Common Tools *x.x*\tomcat *x.x*\webapps\rtmBrowser\forms
RM_Install\RM\rtmBrowser \jscript\	*RM_Install*\Common Tools *x.x*\tomcat *x.x*\webapps\rtmBrowser\jscript\
RM_Install\RM\rtmBrowser \jscripts\	*RM_Install*\Common Tools *x.x*\tomcat *x.x*\webapps\rtmBrowser\jscripts\

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.

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).
In case you are installing a **patch**, this is the directory to which you backed up your rtmBrowser directory tree (refer to chapter).

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:\rtmBrowser12.7.1_Backup\html`
to
`RM_Install\Common Tools #.#\tomcat\#.#\webapps\rtmBrowser\html`.

Updating a Dimensions CM/RM Integration

If you had an integration between Dimensions CM and Dimensions RM 11.x, you must modify the integration in order for it to work with Dimensions RM 12.7.1 or newer.

To update a Dimensions CM/RM integration:

1   Open the following sql file in a text editor:

    RM_Install`\Dimensions\RM\sql\upgrade_cmrm_integration_for_12.1.sql`

2   Edit the following line replacing *RM* with the name of the Dimensions RM Oracle database:

    `C_DB_NAME CONSTANT VARCHAR2(32) := '`*RM*`';`

3   Edit the following line replacing *8080* with the Dimensions RM Tomcat port:

    `C_PORT CONSTANT VARCHAR2(5) := '`*8080*`';`

4   Save your changes to the sql file.

5   Open an SQL Plus or SQL Developer connection to the Oracle database for the Dimensions CM integration.

NOTE By default, the database is named **cm_typical** and there is a user ID of the same name that has the required permissions.

6   Run the sql script.

TIP See the comments in the sql file for details about what the script does.

Quickly Checking the Upgraded Dimensions RM Server

Please see the checks for a fresh installation documented in chapter "Quickly Checking the Installed and Configured Dimensions RM Server" on page 92 and ensure that those appropriate to an upgrade installation can be performed.

Chapter 7
Additional Functions

Working with Secure Socket Layers

Secure Socket Layers (SSL) is an advanced security feature that allows web servers to provide resource protection using the following methods:

- **Encryption.** Allows you to keep the information that passes between the Web server and a client such as a Web browser, RM Import, or RM Import Designer confidential.

- **Data Integrity Protection.** Provides the means for protecting information that passes between the Web server and a client such as a Web browser, RM Import, or RM Import Designer from being altered by a third party.

Configuration Overview

For using Secure Socket Layers with Dimensions RM, you need to have the certificate of the web server in PFX and CER format.

For details on importing the certificate to IIS, see chapter "Importing a PFX Certificate into Microsoft IIS" on page 134.

If you are not using IIS, see chapter "Importing a PFX Certificate into Windows" on page 134.

> **NOTE**
>
> - If you do not have any certificate for the Web server, you can either obtain a certificate from a Certification Authority or a use self-signed certificate.
>
> - If you use a self-signed certificate, note that you have to make the Certification Authority known to your client machines by importing the certificate on each client machine.
>
> - All certificates in the Certification Path must be known and trusted.
>
> - You must have an administrative session (e.g. through Remote Desktop) on the Dimensions RM server.
>
> - PFX certificates may have these file extensions:
>   - pfx
>   - p12
> - CER certificates may have these file extensions:
>   - cer
>   - crt

Importing the Dimensions RM Server Certificate

To import the Dimensions RM certificate, it must be available in CER and PFX format. For details, see these chapters:

- **CER Format:**
  - "Exporting Certificates to CER Format from the Management Console" on page 136 or

- "Exporting Certificates to CER Format from IIS" on page 137.

■ **PFX Format:**

- "Exporting Certificates to PFX Format from the Management Console" on page 138 or

- "Exporting Certificates to PFX Format from IIS" on page 139.

IMPORTANT! Before you start, ensure that you have the alias and password of the PFX file. Alias and password are required for importing the certificate into the SSL keystore (e.g. sample-ssl.jks). To retrieve the alias of the PFX file, see chapter "Retrieving the Alias from a PFX File" on page 143.

To import the certificate, do the following:

1 Stop the **Micro Focus Common Tomcat** service. To stop the service, follow these steps:

a Enter `services.msc` in the command prompt and press **Enter**.

b In the list, select **Micro Focus Common Tomcat**.

c Click ■.

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 (x86)\Micro Focus\Dimensions 12.7.1*.

■ Replace *#.#.#.#* with the Common Tools version number, e.g. *1.8.3.0*.

■ Replace *#.#* with the Java version number, e.g. 8.0.

The complete set command may look like this:

`set path=%path%;"`*`C:\Program Files (x86)\Micro Focus\Dimensions`*` 12.7 .1\Common Tools `*`1.8.3.0`*`\jre\`*`8.0`*`\bin"`

4 If Micro Focus Common Tomcat is not installed on drive C:, change to the drive it is installed. If this is drive E, type `E:` and press **Enter**.

5   Type the following command (all on one line) and press **Enter:**
cd *RM_Install*\Common Tools *#.#.#.#*\tomcat*#.#*\conf

> **NOTE**
>
> ▪ Replace *RM_Install* with the path to the Dimensions directory, e.g. *C:\Program Files (x86)\Micro Focus\Dimensions 12.7.1*.
>
> ▪ Replace **#.#.#.#** with the Common Tools version number, e.g. 1.8.3.0.
>
> ▪ Replace **#.#** with the Tomcat version number, e.g. 8.5.
>
> A complete path may look like this:
>
> *C:\Program Files (x86)\Micro Focus\Dimensions 12.7.1*\Common Tools *1.8.3.0*\tomcat*8.5*\conf

6   Type the following command (all on one line) and press **Enter**:
keytool -importkeystore
-srckeystore *PfxPath* -srcstorepass *PFXPassword*
-srcalias *PFXALIAS* -srcstoretype pkcs12
-destkeystore *SSLKeystore* -deststorepass *SSLStorePassword*
-destalias *SSLAlias* -deststoretype JKS

> **NOTE**
>
> ▪ Replace *PfxPath* with the path and file name to the PFX file, e.g. *C:\Certificates\MyCertificate.pfx*. If the path contains spaces, surround the path with double quotes.
>
> ▪ Replace *PFXALIAS* with the alias used in the PFX file. To retrieve the alias, see chapter "Retrieving the Alias from a PFX File" on page 143.
>
> ▪ Replace *PFXPassword* with the password of the PFX file.
>
> ▪ Replace *SSLKeystore* with the keystore specified in the server.xml file. The default is *sample-ssl.jks*.
>
> ▪ Replace *SSLAlias* with a unique name (e.g. rtm) which you use to reference the certificate from the server.xml file.
> **The alias must be all lowercase.**
>
> ▪ Replace *SSLStorePassword* with the password for the keystore.
> The default password for the sample-ssl.jks keystore is: **serena**
>
> The complete keytool command may look like this (all on one line):
>
> keytool -importkeystore
> -srckeystore *"C:\My Certificates\MyCertificate.pfx"*
> -srcstorepass *topsecret*
> -srcalias *1*
> -srcstoretype pkcs12
> -destkeystore *sample-ssl.jks*
> -deststorepass *serena*
> -destalias *rtm*
> -deststoretype JKS

7   Type the following command and press **Enter:**
```
keytool -keypasswd -keystore SSLKeystore -alias SSLAlias
-keypass PFXPassword
-storepass SSLStorePassword -new SSLStorePassword
```

> **NOTE**
>
> ■ Replace *SSLKeystore* with the keystore specified in the server.xml file. The default is *sample-ssl.jks*.
>
> ■ Replace *SSLAlias* with the alias you used in the previous step for the `-destalias` parameter (e.g. *rtm*).
>
> ■ Replace *PFXPassword* with the password of the PFX file.
>
> ■ Replace *SSLStorePassword* with the password for the keystore.
> The default password for the sample-ssl.jks keystore is: **serena**
> Note that the password for the keystore and for the certificate must be identical, hence the same password for the `-storepass` and `-new` parameters.
>
> The complete keytool command may look like this (all on one line):
>
> ```
> keytool -keypasswd -keystore sample-ssl.jks -alias rtm
> -keypass topsecret -storepass serena -new serena
> ```

8   Type the following command and press **Enter:**
```
cd ..\..\..\jre\8.0\lib\security
```

9   Type the following command (all on one line) and press **Enter**:
```
keytool -import -trustcacerts
-keystore cacerts -storepass StorePassword
-alias Alias -file CerPath
```

> **NOTE**
>
> ■ Replace *StorePassword* with the password for the keystore.
> The default password for the cacerts keystore is: **changeit**
>
> ■ Replace *Alias* with a unique name (e.g. RTM) which you use to reference the certificate from the server.xml file.
>
> ■ 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 cacerts -storepass changeit
> -alias RTM -file "C:\My Certificates\MyCert.cer"
> ```

10   Answer see the message **Trust this certificate? [no]**: Type **yes** and press **Enter**.

11   You receive the message **Certificate was added to keystore**.

12   Repeat steps 10-12 for all certificates in the certification path.

13   Execute the steps of chapter .

14   Ensure that the **Micro Focus Common Tomcat** service is running.

Modifying the Server.xml File

The server.xml file is a configuration file for Micro Focus Common Tomcat in XML format. This file can be read and edited with a plain text editor, e.g. Notepad. **Do not** open this file with a text processor (e.g. MS Word).

To configure SSL in the server.xml file, do the following:

1   Ensure that the **Micro Focus Common Tomcat** service is turned off. To stop the service, follow these steps:

    a   Enter `services.msc` in the command prompt and press **Enter**.

    b   In the list, select **Micro Focus Common Tomcat**.

    c   Click ■.

2   Open *RM_Install*\Common Tools *#.#.#.#*\tomcat*#.#*\conf\server.xml with a text editor, e.g. Notepad.

> **NOTE**
>
> ■   Replace *RM_Install* with the path to the Dimensions directory, e.g. *C:\Program Files (x86)\Micro Focus\Dimensions 12.7.1*.
>
> ■   Replace **#.#.#.#** with the Common Tools version number, e.g. 1.8.3.0.
>
> ■   Replace **#.#** with the Tomcat version number, e.g. 8.5.
>
> A complete path may look like this:
>
> *C:\Program Files (x86)\Micro Focus\Dimensions* 12.7.1\Common Tools *1.8.3.0*\tomcat*8.5*\conf\server.xml

3   Find the following Connector tag:

```
<Connector port="8080" protocol="HTTP/1.1"

connectionTimeout="20000"

redirectPort="8443"

socket.txBufSize="262144"

server="Unknown Web Server/1.0" />
```

4   Surround it with comments, so it looks like this:

```
<!--

<Connector port="8080" protocol="HTTP/1.1"

connectionTimeout="20000"

redirectPort="8443"

socket.txBufSize="262144"

server="Unknown Web Server/1.0" />

-->
```

5   Locate the connectors for port 8443 and 8543 and change the keyAlias value to the alias you used for your server when importing the certificate into the sample-ssl.jks keystore. In the example, that would be ***rtm***. So the connector for port 8443 may

look like this:

```
<Connector port="8443" SSLEnabled="true"
scheme="https" secure="true" sslProtocol="TLS" sslEnabledProtocols="TLSv1.2,TLSv1.1,TLSv1"
maxHttpHeaderSize="8192"
maxThreads="150" minSpareThreads="25"
enableLookups="false" disableUploadTimeout="true"
acceptCount="100"
socket.txBufSize="262144"
keystoreFile="conf/sample-ssl.jks" keystorePass="serena" keyAlias="rtm"
truststoreFile="conf/sample-ssl.jks"
truststorePass="serena"
clientAuth="false" />
```

6 Ensure that both connectors are **not surrounded** with **<!--** and **-->**.

7 Save the file.

8 Start the **Micro Focus Common Tomcat** service. To start the service, follow these steps:

   a Enter `services.msc` in the command prompt and press **Enter**.

   b In the list, select **Micro Focus Common Tomcat**.

   c Click ▶ .

9 After Micro Focus Common Tomcat started up, Dimensions RM is available under this URL: https://*my-server*:8443/rtmBrowser/

Updating the Dimensions RM Server Certificate

Updating of the Dimensions RM certificate may be required to prevent certificate expiration, which may lead to error messages and functionality becoming unavailable.

To update the Dimensions RM certificate, it must be available in CER and PFX format. For details on retrieving the certificate, see these chapters:

- **CER Format:**
  - "Exporting Certificates to CER Format from the Management Console" on page 136 or
  - "Exporting Certificates to CER Format from IIS" on page 137.

- **PFX Format:**
  - "Exporting Certificates to PFX Format from the Management Console" on page 138 or
  - "Exporting Certificates to PFX Format from IIS" on page 139.

🛈 **IMPORTANT!** Before you start, ensure that you have the alias and password of the PFX certificate. Alias and password are required for importing the certificate into the SSL keystore (e.g. sample-ssl.jks). To retrieve the alias of the PFX file, see chapter "Retrieving the Alias from a PFX File" on page 143.

To update the certificate, do the following:

1 Stop the **Micro Focus Common Tomcat** service. To stop the service, follow these steps:

    a Enter `services.msc` in the command prompt and press **Enter**.

    b In the list, select **Micro Focus Common Tomcat**.

    c Click ■

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 (x86)\Micro Focus\Dimensions 12.7.1*.
>
> - Replace **#.#.#.#** with the Common Tools version number, e.g. *1.8.3.0*.
>
> - Replace **#.#** with the Java version number, e.g. 8.0.
>
> The complete set command may look like this:
>
> `set path=%path%;"`*`C:\Program Files (x86)\Micro Focus\Dimensions`*` 12.7`
> `.1\Common Tools `*`1.8.3.0`*`\jre\`*`8.0`*`\bin"`

4 If Micro Focus Common Tomcat is not installed on drive C:, change to the drive it is installed. If this is drive E, type `E:` and press **Enter**.

5 Type the following command (all on one line) and press **Enter:**
`cd `*`RM_Install`*`\Common Tools `*`#.#.#.#`*`\tomcat\`*`#.#`*`\conf`

> **NOTE**
>
> - Replace *RM_Install* with the path to the Dimensions directory, e.g. *C:\Program Files (x86)\Micro Focus\Dimensions 12.7.1*.
>
> - Replace **#.#.#.#** with the Common Tools version number, e.g. 1.8.3.0.
>
> - Replace **#.#** with the Tomcat version number, e.g. 8.5.
>
> A complete path may look like this:
>
> *C:\Program Files (x86)\Micro Focus\Dimensions 12.7.1*\Common Tools *1*
> *.8.3.0*\tomcat*8.5*\conf

6 Type the following command (all on one line) and press **Enter**:
`Notepad server.xml`

7 Locate the connector that is used for your HTTPS connection and take a note of the keystore file, the keystore password and the alias. see the marked parts in the example below:

```
<Connector port="8443" SSLEnabled="true" scheme="https"
secure="true" sslProtocol="TLS"
sslEnabledProtocols="TLSv1.2,TLSv1.1,TLSv1" maxHttpHeaderSize="8192"
maxThreads="150" minSpareThreads="25" enableLookups="false"
disableUploadTimeout="true" acceptCount="100"
socket.txBufSize="262144" keystoreFile="conf/sample-ssl.jks"
```

```
keystorePass="serena" keyAlias="rmserver" truststoreFile="conf/
sample-ssl.jks" truststorePass="serena" clientAuth="false" />
```

> **NOTE** The above example provides the following data:
>
> ■ **keystoreFile:** The relative path to the keystore. This path relates to Tomcat's root directory (e.g.
> `C:\Program Files (x86)\Micro Focus\Dimensions 12.7.1\Common Tools 1.8.3.0\tomcat\8.5)`. So the file name would be **sample-ssl.jks**.
>
> ■ **keystorePass:** The password for the keystore; in the above example it is **serena**.
>
> ■ **keyAlias:** The alias of the certificate; in the above example it is **rmserver**.
>
> The complete set command may look like this:
>
> ```
> set path=%path%;"C:\Program Files (x86)\Micro Focus\Dimensions 12.7.1\Common Tools 1.8.3.0\jre\8.0\bin"
> ```

8 Change back to the command prompt.

9 Type the following command (all on one line)and press **Enter:**
```
keytool -delete -alias keyAlias
-keystore keystoreFile
-storepass keystorePass
```

> **NOTE**
>
> ■ Replace *keyAlias* with the alias you wrote down from the server.xml file.
>
> ■ Replace *keystoreFile* with the keystore you wrote down from the server.xml file.
>
> ■ Replace *keystorePass* with the keystore password you wrote down from the server.xml file.
>
> The complete keytool command may look like this (all on one line):
>
> ```
> keytool -delete -alias rmserver
> -keystore sample-ssl.jks -storepass serena
> ```

10 Type the following command (all on one line) and press **Enter**:
```
keytool -importkeystore
-srckeystore PfxPath -srcstorepass PFXPassword
-srcalias PFXALIAS -srcstoretype pkcs12
-destkeystore SSLKeystore -deststorepass SSLStorePassword
-destalias SSLAlias -deststoretype JKS
```

NOTE

- Replace *PfxPath* with the path and file name to the PFX file, e.g. *C:\Certificates\MyCertificate.pfx*. If the path contains spaces, surround the path with double quotes.

- Replace *PFXALIAS* with the alias used in the PFX file. To retrieve the alias, see chapter "Retrieving the Alias from a PFX File" on page 143.

- Replace *PFXPassword* with the password of the PFX file.

- Replace *SSLKeystore* with the keystore specified in the server.xml file. The default is *sample-ssl.jks*.

- Replace *SSLAlias* with a unique name (e.g. rtm) which you use to reference the certificate from the server.xml file.
  The alias must be all lowercase.

- Replace *SSLStorePassword* with the password for the keystore.
  The default password for the sample-ssl.jks keystore is: **serena**

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

```
keytool -importkeystore
-srckeystore "C:\My Certificates\MyCertificate.pfx"
-srcstorepass topsecret
-srcalias 1
-srcstoretype pkcs12
-destkeystore sample-ssl.jks
-deststorepass serena
-destalias rtm
-deststoretype JKS
```

11   Type the following command and press **Enter:**
```
keytool -keypasswd -keystore SSLKeystore -alias SSLAlias
-keypass PFXPassword
-storepass SSLStorePassword -new SSLStorePassword
```

> **NOTE**
>
> ■ Replace *SSLKeystore* with the keystore specified in the server.xml file. The default is *sample-ssl.jks*.
>
> ■ Replace *SSLAlias* with the alias you used in the previous step for the -destalias parameter (e.g. *rtm*).
>
> ■ Replace *PFXPassword* with the password of the PFX file.
>
> ■ Replace *SSLStorePassword* with the password for the keystore.
>   The default password for the sample-ssl.jks keystore is: **serena**
>   Note that the password for the keystore and for the certificate must be identical, hence the same password for the -storepass and -new parameters.
>
> The complete keytool command may look like this (all on one line):
>
> ```
> keytool -keypasswd -keystore sample-ssl.jks -alias rtm
> -keypass topsecret -storepass serena -new serena
> ```

12   Type the following command and press **Enter:**
```
cd ..\..\..\jre\8.0\lib\security
```

13   Type the following command (all on one line) and press **Enter**:
```
keytool -list -v
-keystore cacerts -storepass StorePassword >certs.txt
```

> **NOTE** Replace *StorePassword* with the password for the keystore. The default is **changeit**
>
> The complete keytool command may look like this:
>
> ```
> keytool -list -v -keystore cacerts -storepass changeit >certs.txt
> ```

14   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.

15   Locate the certificate in the file (e.g. by searching for the server name). Verify that the certificate you located is valid (by checking the validity date). Search for **Valid from:** to locate the validity range. The validity range looks similar to this example:
```
Valid from: Wed Feb 07 21:21:09 CST 2018 until: Mon Feb 10 21:21:09 CST 2020
```

16   Locate the line starting with **Alias name** and write down the value. In this example, the alias name is rmserver: **Alias name:** *rmserver*

17 Type the following command and press **Enter:**
```
keytool -delete -keystore cacerts -storepass StorePassword
-alias Alias
```

> **NOTE**
>
> ■ Replace *Alias* with the alias you used retrieved from the certs.txt file, (e.g. *rmserver*).
>
> ■ Replace *StorePassword* with the password for the keystore.
> The default password for the sample-ssl.jks keystore is: **changeit**
>
> The complete keytool command may look like this (all on one line):
>
> ```
> keytool -delete -keystore cacerts -alias rmserver
> -storepass changeit
> ```

18 Type the following command (all on one line) and press **Enter**:
```
keytool -import -trustcacerts
-keystore cacerts -storepass StorePassword
-alias Alias -file CerPath
```

> **NOTE**
>
> ■ Replace *StorePassword* with the password for the keystore.
> The default password for the cacerts keystore is: **changeit**
>
> ■ Replace *Alias* with a unique name (e.g. RTM) which you use to reference the certificate from the server.xml file.
>
> ■ 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 cacerts -storepass changeit
> -alias RTM -file "C:\My Certificates\MyCert.cer"
> ```

19 Answer see the message **Trust this certificate? [no]**: Type **yes** and press **Enter**.

20 You receive the message **Certificate was added to keystore**.

21 Repeat steps 16-21 for all certificates in the certification path.

22 Start the **Micro Focus Common Tomcat** service. To stop the service, follow these steps:

   a Enter `services.msc` in the command prompt and press **Enter**.

   b In the list, select **Micro Focus Common Tomcat**.

   c Click ▷

Updating SSO Certificates

When using Single Sign On (SSO), it may be required to update the certificates in Micro Focus Common Tomcat to prevent login failure after certificate expiration.

For import, you need the following certificates in CER format:

- Federation Server certificate (*fedsrv.cer*)

- STS certificate (*sts.cer*)

- SSO Gatekeeper certificate (*gatekeeper.cer*)

The certificates are imported into the keystores `keystore.jks` and `truststore.jks` at *RM_Install*\Common Tools *#.#.#.#*\tomcat*#.#*\alfssogatekeeper\conf

> **CAUTION!** During the update procedure, you will delete the existing certificates from the keystores and then import the new certificates.
>
> **It is strongly advised to create backups** of `keystore.jks` and `truststore.jks` before starting the update process.

To update the certificates, execute these steps:

1 Stop the **Micro Focus Common Tomcat** service. To stop the service, follow these steps:

    a Enter `services.msc` in the command prompt and press **Enter**.

    b In the list, select **Micro Focus Common Tomcat**.

    c Click ▇

2 Open a command prompt.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 (x86)\Micro Focus\Dimensions 12.7.1*.
>
> - Replace **#.#.#.#** with the Common Tools version number, e.g. *1.8.3.0*.
>
> - Replace **#.#** with the Java version number, e.g. 8.0.
>
> The complete set command may look like this:
>
> set path=%path%;"*C:\Program Files (x86)\Micro Focus\Dimensions* 12.7 .1\Common Tools *1.8.3.0*\jre*8.0*\bin"

3 Type the following command (all on one line)and press **Enter:**
cd *RM_Install*\Common Tools *#.#.#.#*\tomcat*#.#*\alfssogatekeeper\conf

> **NOTE**
>
> ■ Replace *RM_Install* with the path to the Dimensions directory, e.g.
>   *C:\Program Files (x86)\Micro Focus\Dimensions 12.7.1*.
>
> ■ Replace **#.#.#.#** with the Common Tools version number, e.g. 1.8.3.0.
>
> ■ Replace **#.#** with the Tomcat version number, e.g. 8.5.
>
> A complete path may look like this:
>
> *C:\Program Files (x86)\Micro Focus\Dimensions 12.7.1*\Common Tools *1*
> *.8.3.0*\tomcat*8.5*\alfssogatekeeper\conf

4 Type the following command (all on one line)and press **Enter:**
keytool -delete -alias gatekeeper
-keystore keystore.jks
-storepass *changeit*

> **NOTE** If you changed the password for keystore.jks, replace *changeit* with the
> actual password.

5 Type the following command (all on one line)and press **Enter:**
keytool -import -trustcacerts
-keystore keystore.jks -storepass *changeit*
-alias gatekeeper -file *gatekeeper.cer*

> **NOTE**
>
> ■ If you changed the password for keystore.jks, replace *changeit* with the
>   actual password.
>
> ■ Replace *gatekeeper.cer* with the full path to the Gatekeeper certificate.

6 Verify that the command prompt shows this message:
Certificate was added to keystore.

7 Type the following command (all on one line)and press **Enter:**
keytool -delete -alias sts
-keystore truststore.jks
-storepass *changeit*

> **NOTE** If you changed the password for truststore.jks, replace *changeit* with
> the actual password.

8 Type the following command (all on one line)and press **Enter:**
keytool -import -trustcacerts

```
-keystore truststore.jks -storepass changeit
-alias sts -file sts.cer
```

> **NOTE**
>
> - If you changed the password for `truststore.jks`, replace *changeit* with the actual password.
>
> - Replace *sts.cer* with the full path to the STS certificate.

9 Verify that the command prompt shows this message:
Certificate was added to keystore.

10 Type the following command (all on one line)and press **Enter:**
```
keytool -delete -alias fedsrv
-keystore truststore.jks
-storepass changeit
```

> **NOTE** If you changed the password for `truststore.jks`, replace *changeit* with the actual password.

11 Type the following command (all on one line)and press **Enter:**
```
keytool -import -trustcacerts
-keystore truststore.jks -storepass changeit
-alias fedsrv -file fedsrv.cer
```

> **NOTE**
>
> - If you changed the password for `truststore.jks`, replace *changeit* with the actual password.
>
> - Replace *fedsrv.cer* with the full path to the Federation Server certificate.

12 Verify that the command prompt shows this message:
Certificate was added to keystore.

13 Start the **Micro Focus Common Tomcat** service. To stop the service, follow these steps:

   a Enter `services.msc` in the command prompt and press **Enter**.

   b In the list, select **Micro Focus Common Tomcat**.

   c Click ▷

Importing Certificates on the Client

When using self-signed certificates, these certificates must be imported on the client machines to allow HTTPS connections.

Importing Certificates with Internet Explorer / Edge / Chrome

To import a certificate, execute these steps:

1 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 **Trusted Root Certification Authorities**.

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

11 Click **Next**.

12 Click **Browse...** to open the file selection dialog.

13 Select the certificate and click **Open**.

14 Click **Next**.

15 Ensure that option **Place all certificates in the following store** is selected and Certificate store contains the text **Trusted Root Certification Authorities**. If it does not, do the following:

    a Click **Browse...** to open the **Select Certificate Store** dialog.

    b Select **Trusted Root Certification Authorities** from the list.

    c Click **OK** to close the **Select Certificate Store** dialog and use the selected value in the **Certificate Import Wizard**.

16 Click **Next**.

17 Click **Finish** to import the certificate.

18 Restart Internet Explorer, Edge, or Chrome respectively.

Importing Certificates with Firefox

To import a certificate, execute these steps:

1 Start Firefox if it is not already running.

2 Click ☰ to open the settings menu.

3 Select **Options** to open the **Options** tab.

4 Select **Advanced** in the left pane.

5 In the right frame, select **Certificates**.

6 Click **View Certificates** to open the **Certificate Manager** dialog.

7 Select the **Authorities** tab.

8 Click **Import...** to open the certificate selection dialog.

9 Select one or several certificates to import and click **Open**. This opens the **Downloading Certificate** dialog.

10 Select the **Trust this CA to identify websites** option.

11 To verify that this is the certificate is correct, do the following:

    a Click **View** to open the certificate in the **Certificate Viewer** dialog.

    b Verify that this is the certificate you want to import.

    c Click **Close** to close the **Certificate Viewer** dialog.

12 Click **OK** to import the certificate.

13 Click **OK** to close the **Certificate Manager** dialog.

14 Restart Firefox.

Configuring Secure Cookies

When using Dimensions RM in a secure area, you may want to prevent that data stored in cookies (e.g. session ID) can be retrieved by an attacker. This can be achieved by configuring secure cookies.

NOTE

- Secure cookies require that Dimensions RM is accessed through a secure channel (usually HTTPS with TLS enabled).

- With a man-in-the-middle attack, secure cookies could be overwritten

To configure secure cookies, do the following:

1 Stop the **Micro Focus Common Tomcat** service.

2 Open *RM_Install*\Common Tools *#.#.#.#*\tomcat*#.#*\webapps\rtmBrowser\ WEB-INF\web.xml with a text editor, e.g. Notepad.

3 Search for the **session-config** node.

4 Locate the **secure** node and change its value to **true**. This should result into the following XML.

```
<session-config>
  <cookie-config>
    <secure>true</secure>
  </cookie-config>
</session-config>
```

5 Save the file.

6 Start the **Micro Focus Common Tomcat** service.

Configuring HTTP Strict Transport Security

HTTP Strict Transport Security (HSTS) forbids Tomcat to use the HTTP protocol. Configuring HSTS helps to protect against protocol downgrade attacks (connect with HTTP instead of HTTPS) and cookie hijacking.

To configure HTTP Strict Transport Security, do the following:

1 Stop the **Micro Focus Common Tomcat** service.

2 Open *RM_Install*\Common Tools *#.#.#.#*\tomcat*#.#*\webapps\rtmBrowser\ WEB-INF\web.xml with a text editor, e.g. Notepad.

3 Search for the following text:
<filter-name>httpHeaderSecurity</filter-name>.

4 Remove the following content:

```
<!--
<filter>
<filter-name>httpHeaderSecurity</filter-name>
<filter-class>org.apache.catalina.filters.HttpHeaderSecurityFilter</filter-class>
<async-supported>true</async-supported>
</filter>
-->
```

5 Add the following content:

```
<filter>
<filter-name>httpHeaderSecurity</filter-name>
<filter-class>org.apache.catalina.filters.HttpHeaderSecurityFilter</filter-class>
<async-supported>true</async-supported>
<init-param>
<param-name>antiClickJackingEnabled</param-name>
<param-value>false</param-value>
</init-param>
</filter>

<filter-mapping>
<filter-name>httpHeaderSecurity</filter-name>
```

```
<url-pattern>/*</url-pattern>
<dispatcher>REQUEST</dispatcher>
</filter-mapping>
```

6   Save the file.

7   Start the **Micro Focus Common Tomcat** service.

Configuring Tomcat

Preparing Configuration

To allow modification of Tomcat specific settings, do the following:

1   In Windows Explorer, navigate to the following path:
RM_Install\Common Tools 1.8.3.0\tomcat\8.5\bin

> **NOTE**
>
> Replace *RM_Install* with the path to the Dimensions directory, e.g.
> *C:\Program Files (x86)\Micro Focus\Dimensions 12.7.1*.

2   Create a copy of the file tomcat8w.exe.

3   Rename the copy to MicroFocusTomcatw.exe.

Configuring Memory Pool

By configuring Tomcat's memory pool, Tomcat can use more memory for its operations. A high memory pool value allows to download larger files for example. If Tomcat does not start, a smaller memory pool value should be configured.

To configure the memory pool:

1   Ensure that the steps in chapter have been executed.

2   Start MicroFocusTomcatw.exe. This opens the **Micro Focus Common Tomcat** Properties dialog.

3   Select the **Java** tab.

4   Change the value in the **Memory pool** boxes to the desired values.

If Tomcat can't start:

- **Initial memory pool:** 1024
- **Maximum memory pool:** 1024

To allow downloading larger files:

- **Initial memory pool:** 640
- **Maximum memory pool:** desired value, e.g. 1536

Default Values:

- **Initial memory pool:** 640

- **Maximum memory pool:** 1280

5 Click **OK**.

6 Restart the **Micro Focus Common Tomcat** service.

Configuring LDAP

Dimensions RM supports multiple login sources, including Lightweight Directory Access Protocol (LDAP). For information about configuring LDAP, see the *Dimensions RM Administrator's Guide*.

Appendix A
Handling Certificates

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 "Importing a PFX Certificate into Microsoft IIS" on page 134. 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 138).

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 138).

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 136).

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).

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

12 Click **Next**.

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

14 Select the following options:

- **Include all certificates in the certification path if possible**

- **Export all extended properties**

15 Click **Next**.

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

17 Click **Next**.

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

19 Select the target directory and specify a file name.

20 Click **Save**.

21 Click **Next**.

22 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 142).

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 (x86)\Micro Focus\Dimensions 12.7.1*.
>
> ■   Replace *#.#.#.#* with the Common Tools version number, e.g. *1.8.3.0*.
>
> ■   Replace *#.#* with the Java version number, e.g. 8.0.
>
> The complete set command may look like this:
>
> `set path=%path%;"`*`C:\Program Files (x86)\Micro Focus\Dimensions`*` 12.7`
> `.1\Common Tools `*`1.8.3.0`*`\jre\`*`8.0`*`\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 (x86)\Micro Focus\Dimensions 12.7.1*.
>
> ■ Replace ***#.#.#.#*** with the Common Tools version number, e.g. *1.8.3.0*.
>
> ■ Replace ***#.#*** with the Java version number, e.g. 8.0.
>
> The complete set command may look like this:
>
> `set path=%path%;"`*`C:\Program Files (x86)\Micro Focus\Dimensions`*` 12.7`
> `.1\Common Tools `*`1.8.3.0`*`\jre\`*`8.0`*`\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 (x86)\Micro Focus\Dimensions 12.7.1*.
>
> ■   Replace **#.#.#.#** with the Common Tools version number, e.g. *1.8.3.0*.
>
> ■   Replace **#.#** with the Java version number, e.g. 8.0.
>
> The complete set command may look like this:
>
> `set path=%path%;"`*C:\Program Files (x86)\Micro Focus\Dimensions* `12.7`
> `.1\Common Tools `*1.8.3.0*`\jre\`*8.0*`\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*

Appendix B

Migrating Oracle to MS SQL Server

Prerequisites

To allow migration from Oracle to Microsoft SQL Server, the following prerequisites must be met:

- MS SQL Server 2016 SP1 must be installed (see chapter "Installing and Configuring MS SQL Server" on page 45).

- SQL Server Management Studio must be installed (see chapter "Installing SQL Server Management Studio" on page 47).

- An empty MS SQL database must exist (see chapter "Creating a Database Instance" on page 47).

- A Dimensions RM server instance which connects to the MS SQL Server must be exist

- Oracle client must be installed on the server running MS SQL Server 2016 SP1 (see chapters "The Administrator Oracle Client" on page 34 and "Oracle 32-Bit client Installation" on page 39).

- Ensure that the firewall port for the Oracle client is open. By default, this is port 1521.

- Ensure that you have the passwords for these Oracle users:

  - ICADMIN (identical with the password for ICADMIN used in RM Manage)

  - Dimensions RM instances you want to migrate(e.g. RMDEMO)

Testing Connection to the Oracle Database

To test the connection to the Oracle database, do the following:

1 Open a command prompt.

2 Type `sqlplus` and press **Enter**.

3 Type the user name and database name in this format **user@database**, e.g. `icdba@orcl` and press **Enter**.

4 Type the password and press **Enter**. Note that the cursor does not move when you type the password.

5 If successful, you will see a message similar to this:
   ```
   Connected to:
   Oracle Database 11g Release 11.2.0.3.0 - 64bit Production
   SQL>
   ```

6 Type `exit` and press **Enter** to disconnect.

7 Repeat steps 3-6 for all Dimensions RM instances you want to migrate.

Migrating to MS SQL Server

The following chapters assume the following:

1 You match all the prerequisites listed in chapter "Prerequisites" on page 146.

2 There are two Dimensions RM servers, one connecting to MS SQL server and one connecting to Oracle.
If you are migrating within an upgrade procedure (using the same Dimensions RM server), the steps to be executed on the Dimensions RM server connecting to Oracle must be omitted.

All actions described in the following chapters are executed on the Dimensions RM server that connects to the MS SQL Server. If actions are executed on the Dimensions RM server connecting to the Oracle database, a special note will be given.

Shutting Down Dimensions RM

On the Dimensions RM server, disable the following services:

- Micro Focus Common Tomcat

- Micro Focus Dimensions RM E-Mail Notification Service

- Micro Focus Dimensions RM Pool Manager

- Micro Focus SyncEngine

NOTE

1 Before shutting down the services, take a note which of these was running.

2 If you have independent servers connecting to MS SQL Server and Oracle, execute above steps on both servers.

Creating the required Accounts

The following steps are executed with RM Manage. For information about RM Manage, see the *Dimensions RM Administrator's Guide*.

TIP To avoid confusion, you might want to use the same passwords for the MS SQL Server accounts as for the Oracle accounts (i.e. ICADMIN, ICDBA, ICPROJECTS, and your Dimensions RM instances).

To create the required accounts, do the following:

1 Start **RM Manage**.

2 Create the ICDBA account. For information on creating the ICDBA account, see chapter *"Creating the ICDBA Account"* in the *Dimensions RM Administrator's Guide*.

3 Create the Dimensions RM instances you want to migrate. Use the same names as on the Dimensions RM server connecting to the Oracle database. For information about creating a Dimensions RM instance, see chapter "Creating a New Instance" in the *Dimensions RM Administrator's Guide*.

Migrating a Dimensions RM Instance to MS SQL Server

Before you start, ensure the following:

- All prerequisites listed in chapter "Prerequisites" on page 146 are met.

- You executed the steps listed in chapter "Creating the required Accounts" on page 147.

- You can connect to the Oracle database (see chapter "Testing Connection to the Oracle Database" on page 146).

Migrating ICADMIN Tables

To migrate ICADMIN tables, do the following:

1 Start **SQL Server Management Studio** and log in as "sa" user.

2 Expand the server node.

3 Expand the **Databases** folder.

4 Expand the **Tables** folder.

5 Right-click the database instance into you wish to import, e.g. *RTM*.

6 From the shortcut menu, select **Tasks** and then **Import Data...**. This opens the **SQL Server Import and Export Wizard**.

7 From the **Data source** box, select **.Net Framework Data Provider for Oracle**.

8 Expand the **Security** section if required.

9 For **User ID**, specify **ICADMIN**.

10 For **Password**, specify the Oracle password for the **ICADMIN** user.

11 Expand the **Source** section if required.

12 For **Data Source**, specify the name under which your Oracle system is listed in your `tnsnames.ora` file, e.g. *PROD_RM*.

13 Click **Next**.

NOTE If you get a message that you require Oracle client 8.1.7 or greater, see chapter "Oracle Client 8.1.7 or greater required" on page 156.

14 From the **Destination** box, select **SQL Server Native Client 11.0**.

15 Verify that the entries for **Server name** and **Database** are correct.

16 Select the **Use SQL Server Authentication** option.

17 For **User name**, enter **ICADMIN**.

18 For **Password**, enter the password for the ICADMIN account.

19 Click **Next**.

20 Ensure that the option **Copy data from one or more tables or views** is selected.

21 Execute the following actions for each table with **ICADMIN** (one table at a time):

    a Select a table (check box next to table name is selected).

    b Click **Edit Mappings...**. This opens the **Transfer Settings** dialog.

    c Select the **Delete rows in existing destination tables** option.

    d Click **OK**.

22 Click **Next**.

23 Ensure that the **Run immediately** option is selected.

24 Click **Next**.

25 Verify that all values (especially for **Source Location** and **Destination Location**) are correct.

26 Click **Finish** to start the import.

27 After the import has been completed, execute the steps described in chapter "Updating Sequences for ICADMIN" on page 149.

Updating Sequences for ICADMIN

To update the sequences for ICADMIN, do the following:

1 Log in to Oracle as user **ICADMIN**.

2 Run the script from chapter "Script for Sequence Retrieval" on page 153.

> **IMPORTANT!** Prior to running the script, replace *Instance* by `ICADMIN`, so you see `WHERE sequence_owner = 'ICADMIN' ORDER BY sequence_name`

3 Start **SQL Server Management Studio** and log in as user **ICADMIN**.

4 Select the database in which you wish to update the sequences.

5 Click **New Query**. This opens an query window.

6 Insert the script from **Script for Sequence Update** into the query window.

7 Copy string from Oracle dbms output (like ADM_PROJECT_IDS=**) to your clipboard (`Ctrl+C`).

8 In the SQL Server Management Studio query window, replace the text *ORACLE_SEQUENCE_DATA* with the Oracle dbms output from the clipboard (`Ctrl+V`).

9 Execute the script.

Migrating RM Instance Tables

The following steps describe how to import a single RM instance. If you need to import several instances, all steps must be executed for each instance.

Before you start, ensure that you executed the steps from the following chapters:

-

-

To migrate RM instance tables, do the following:

1 Start **SQL Server Management Studio** and log in with the user name that is identical to the name of the RM instance, e.g. *RMDEMO*.

2 Expand the server node.

3 Expand the **Databases** folder.

4 Expand the **Tables** folder.

5 Right-click the database instance into you wish to import, e.g. *RTM*.

6 From the shortcut menu, select **Tasks** and then **Import Data...**. This opens the **SQL Server Import and Export Wizard**.

7 From the **Data source** box, select **.Net Framework Data Provider for Oracle**.

8 Expand the **Security** section if required.

9 For **User ID**, specify the RM instance name, e.g. *RMDEMO*.

10 For **Password**, specify the Oracle password for the RM instance.

11 Expand the **Source** section if required.

12 For **Data Source**, specify the name under which your Oracle system is listed in your `tnsnames.ora` file, e.g. *PROD_RM*.

13 Click **Next**.

> **NOTE** If you get a message that you require Oracle client 8.1.7 or greater, see chapter .

14 From the **Destination** box, select **SQL Server Native Client 11.0**.

15 Verify that the entries for **Server name** and **Database** are correct.

16 Select the **Use SQL Server Authentication** option.

17 For **User name**, enter the name of the RM instance, e.g. *RMDEMO*.

18 For **Password**, enter the password for the RM instance.

19 Click **Next**.

20 Ensure that the option **Copy data from one or more tables or views** is selected.

21 Execute the following actions for each table **except** those starting with **RM_ATTRS** and **TEMP** (one table at a time):

  a Select a table (check box next to table name is selected).

  b Click **Edit Mappings...**. This opens the **Transfer Settings** dialog.

  c Select the **Delete rows in existing destination tables** option.

    d Click **OK**.

22   Select all tables, **except** those starting with **RM_ATTRS** and **TEMP**.

> **NOTE** As import may take a lot of server resources, you may import tables in batches (e.g. starting with A-E).

23   Click **Next**.

24   Ensure that the **Run immediately** option is selected.

25   Click **Next**.

26   Verify that all values (especially for **Source Location** and **Destination Location**) are correct.

27   Click **Finish** to start the import. If you are importing in batches, repeat the previous import steps until all tables (**except** those starting with **RM_ATTRS** and **TEMP**) have been imported.

28   Expand the database instance for which you wish to generate the RM_ATTS tables, e.g. *RTM*.

29   Click **New Query**. This opens an query window.

30   Insert the script from chapter "Script for Generating RM_ATTRS Tables and Views" on page 154 into the query window.

31   Execute the script.

32   Right-click the database instance into you wish to import, e.g. *RTM*.

33   From the shortcut menu, select **Tasks** and then **Import Data...**. This opens the **SQL Server Import and Export Wizard**.

34   From the **Data source** box, select **.Net Framework Data Provider for Oracle**.

35   Expand the **Security** section if required.

36   For **User ID**, specify the RM instance name, e.g. *RMDEMO*.

37   For **Password**, specify the Oracle password for the RM instance.

38   Expand the **Source** section if required.

39   For **Data Source**, specify the name under which your Oracle system is listed in your `tnsnames.ora` file, e.g. *PROD_RM*.

40   Click **Next**.

> **NOTE** If you get a message that you require Oracle client 8.1.7 or greater, see chapter "Oracle Client 8.1.7 or greater required" on page 156.

41   From the **Destination** box, select **SQL Server Native Client 11.0**.

42   Verify that the entries for **Server name** and **Database** are correct.

43   Select the **Use SQL Server Authentication** option.

44   For **User name**, enter the name of the RM instance, e.g. *RMDEMO*.

45 For **Password**, enter the password for the RM instance.

46 Click **Next**.

47 Ensure that the option **Copy data from one or more tables or views** is selected.

48 Select all tables, starting with **RM_ATTRS**.

> **NOTE** As import may take a lot of server resources, you may import the RM_ATTRS tables in batches.

49 Click **Next**.

50 Ensure that the **Run immediately** option is selected.

51 Click **Next**.

52 Verify that all values (especially for **Source Location** and **Destination Location**) are correct.

53 Click **Finish** to start the import. If you are importing in batches, repeat the previous import steps until all RM_ATTRS tables have been imported.

54 After the import has been completed, execute the steps described in chapter "Updating Sequences for an RM Instance" on page 152.

Updating Sequences for an RM Instance

Before you start, ensure that you completed chapter "Migrating RM Instance Tables" on page 149.

To update the sequences for an RM instance, do the following:

1 Log in to Oracle as with the user name that is identical to the name of the RM instance, e.g. *RMDEMO*.

2 Run the script from chapter "Script for Sequence Retrieval" on page 153.

> **IMPORTANT!** Prior to running the script, replace *Instance* by the name of the RM instance. So if your RM instance name is RMDEMO, so you see WHERE `sequence_owner = '`*RMDEMO*`' ORDER BY sequence_name`

3 Start **SQL Server Management Studio** and log in with the user name that is identical to the name of the RM instance, e.g. *RMDEMO*.

4 Select the database in which you wish to update the sequences.

5 Click **New Query**. This opens an query window.

6 Insert the script from chapter "Script for Sequence Update" on page 153 into the query window.

7 Copy string from Oracle dbms output (like APPEND_TEXT_ROW_ID=**) to your clipboard (`Ctrl+C`).

8 In the SQL Server Management Studio query window, replace the text *ORACLE_SEQUENCE_DATA* with the Oracle dbms output from the clipboard (`Ctrl+V`).

9 Execute the script.

Scripts

Script for Sequence Retrieval

```
set ECHO ON;
set SERVEROUTPUT ON;
/*Get sequences string from Oracle*/
DECLARE
   v_str VARCHAR2(32000);
BEGIN
   FOR r IN (SELECT sequence_name, last_number FROM all_sequences WHERE
sequence_owner = 'INSTANCE' ORDER BY sequence_name)
LOOP
   IF (v_str IS NOT NULL) THEN
        v_str := v_str || ';';
   END IF;
   v_str := v_str || r.sequence_name || '=' || r.last_number;
END LOOP;
IF (v_str IS NOT NULL) THEN
   v_str := v_str || ';';
END IF;
dbms_output.put_line(v_str);
END;
```

Script for Sequence Update

```
/*Update sequences in MS SQL Server using the string from Oracle*/
BEGIN
   DECLARE
        @seq_txt NVARCHAR(MAX),
        @sql_txt NVARCHAR(4000);
   SET @seq_txt = 'ORACLE_SEQUENCE_DATA';
   DECLARE
```

```
            @stringToSplit NVARCHAR(MAX) = @seq_txt,

            @fname NVARCHAR(1024), @name NVARCHAR(1024), @value
    VARCHAR(1024),

            @pos INT, @pos2 INT;

        WHILE CHARINDEX(';', @stringToSplit) > 0

        BEGIN

            SELECT @pos   = CHARINDEX(';', @stringToSplit);

            SELECT @fname = SUBSTRING(@stringToSplit, 1, @pos - 1);

            SELECT @pos2  = CHARINDEX('=', @fname);

            SELECT @name = SUBSTRING(@fname, 1, @pos2 - 1), @value =
    SUBSTRING(@fname, @pos2 + 1, LEN(@fname));

            IF EXISTS (SELECT * FROM INFORMATION_SCHEMA.SEQUENCES WHERE
    sequence_schema = SCHEMA_NAME() AND sequence_name = @name) BEGIN

                SET @sql_txt = 'ALTER SEQUENCE ' + @name + ' RESTART WITH '
    +  @value;

                EXEC sp_executesql @sql_txt;

            END ELSE BEGIN

                SET @sql_txt = 'CREATE SEQUENCE ' + @name + ' START WITH ' +
    @value;

                EXEC sp_executesql @sql_txt;

            END;

            SELECT @stringToSplit = SUBSTRING(@stringToSplit, @pos + 1,
    LEN(@stringToSplit) - @pos);

        END;

    END;
```

Script for Generating RM_ATTRS Tables and Views

```
BEGIN

    DECLARE

        @class_id INT,

        @attribute_id INT,

        @attribute_type INT,

        @sql_txt NVARCHAR(4000);

    DECLARE cm_cursor CURSOR FOR
```

```
        SELECT class_id FROM class_definition;

    OPEN cm_cursor;

    FETCH NEXT FROM cm_cursor INTO @class_id;

    WHILE @@FETCH_STATUS = 0 BEGIN

        SET @sql_txt = 'CREATE TABLE RM_ATTRS_' + CAST(@class_id AS
NVARCHAR) + ' (CLASS_ID INTEGER NOT NULL, OBJECT_ID INTEGER NOT NULL,
VERSION_ID INTEGER NOT NULL, CONSTRAINT PK_RM_ATTRS_' + CAST(@class_id
AS NVARCHAR) + ' PRIMARY KEY (OBJECT_ID,VERSION_ID))';

        EXEC sp_executesql @sql_txt;

        FETCH NEXT FROM cm_cursor INTO @class_id;

    END;

    CLOSE cm_cursor;

    DEALLOCATE cm_cursor;

    DECLARE attr_cursor CURSOR FOR

        SELECT class_id, attribute_id, attribute_type FROM
attribute_definition WHERE implicit = 0 AND class_id <> -1;

    OPEN attr_cursor;

    FETCH NEXT FROM attr_cursor INTO @class_id, @attribute_id,
@attribute_type;

    WHILE @@FETCH_STATUS = 0 BEGIN

        EXEC Icdefinition__STP_ADD_ATTR_RM_ATTRS @class_id,
@attribute_id, @attribute_type;

        FETCH NEXT FROM attr_cursor INTO @class_id, @attribute_id,
@attribute_type;

    END;

    CLOSE attr_cursor;

    DEALLOCATE attr_cursor;

    EXEC pkg_rm_views__generate_rm_views;

END;
```

Troubleshooting

Oracle Client 8.1.7 or greater required

If you get a message that you require Oracle client 8.1.7 or greater, this may be a permission issue. In this case, do the following:

1   In Windows Explorer, navigate to the Oracle client folder.

2   Right-click the folder and select **Properties**. This opens the **Properties** dialog for the selected folder.

3   Select the **Security** tab.

4   Click **Advanced**. This opens the **Advanced Security Settings** dialog for the selected folder.

5   Click **Add**. This opens the **Permission Entry** dialog for the selected folder.

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

7   Click **Advanced...**. This opens the **Select User or Group** dialog.

8   Click **Find Now**.

9   Select **Authenticated Users** and click **OK**.

10   Click **OK** to close the **Select User or Group** dialog.

11   Ensure that the following settings are selected:

- **Type:** Allow

- **Applies to:** This folder, subfolders and files

12   Select the **Read & execute** option.

13   Click **OK**. This closes the **Permission Entry** dialog for the selected folder.

14   Click **OK** to close the **Advanced Security Settings** dialog for the selected folder.

15   Click **OK** to close the **Properties** dialog for the selected folder.

Index