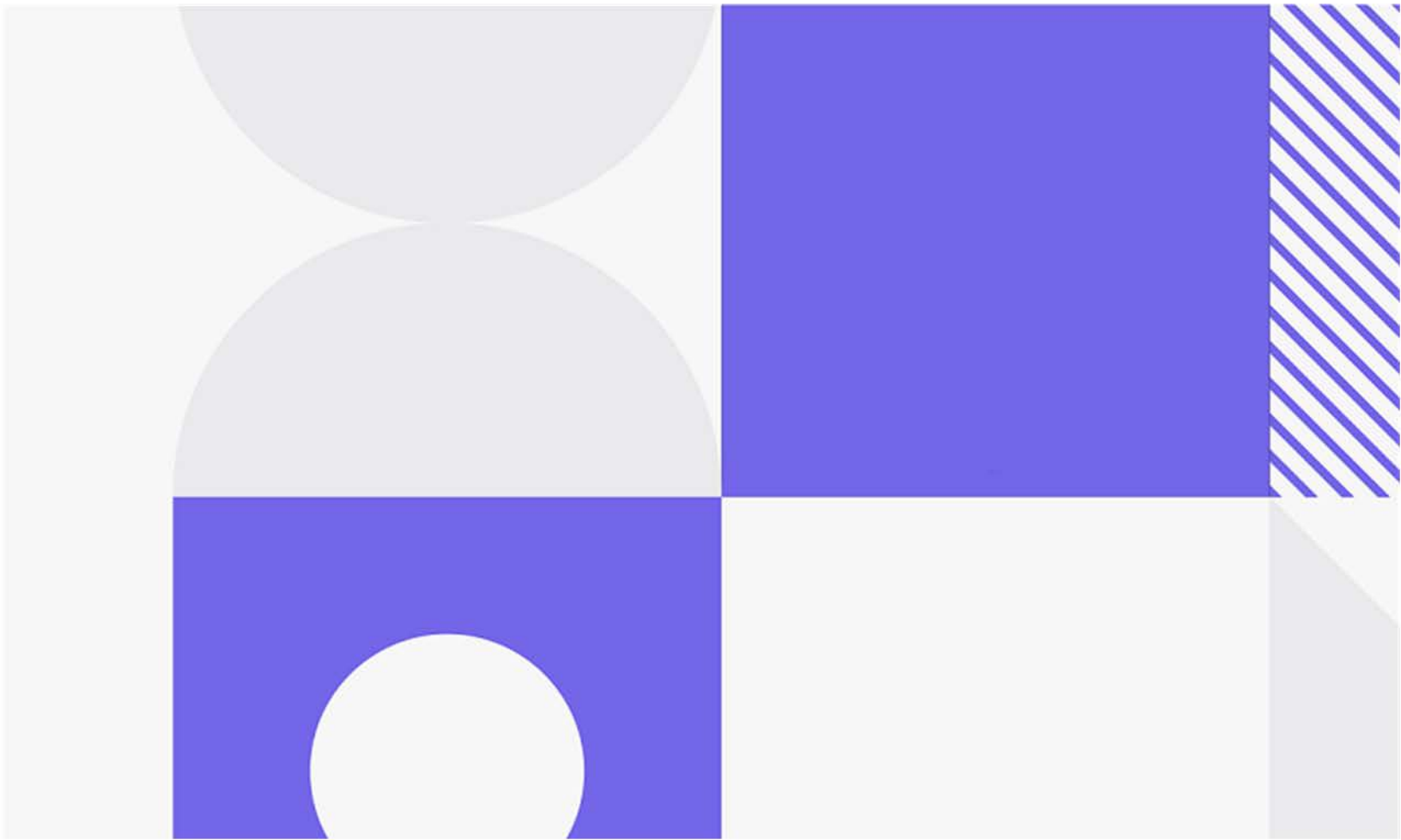


**opentext™**

# Dimensions RM

Software version: 25.2 (13)

## Administrator's Guide



Copyright © 2025 Open Text.

The only warranties for products and services of Open Text and its affiliates and licensors ("Open Text") are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Product version: 25.2 (13)

Last updated: May 11, 2025

# Table of Contents

---

<b>Preface</b> . . . . .	<b>15</b>
Objective . . . . .	15
Edition Status . . . . .	15
Audience. . . . .	15
Typographical Conventions . . . . .	15
Printing Manuals . . . . .	16
Contacting Technical Support . . . . .	16
License and Copyright Information for Third-Party Software . . . . .	17
<b>Chapter 1</b> <b>Dimensions RM Overview.</b> . . . . .	<b>19</b>
The Role of the System Administrator . . . . .	20
The Role of Requirements Management . . . . .	20
Requirement Development . . . . .	20
Reporting and Traceability . . . . .	21
Change Management . . . . .	21
RM Import Designer . . . . .	21
RM Import . . . . .	22
RM Manage. . . . .	23
Class Definition . . . . .	23
Dimensions RM Data Structure . . . . .	23
Dimensions RM Basics . . . . .	24
Users and Groups . . . . .	24
Instance Schemas . . . . .	25
Naming Conventions . . . . .	27
Categories . . . . .	36
Requirement Creation . . . . .	36
Requirement Evolution. . . . .	37
Requirement Views . . . . .	39
Queries . . . . .	41
Query Terminology . . . . .	41
Reports . . . . .	42
Containers . . . . .	42
Collections . . . . .	42
Traceability and Impact Analysis . . . . .	42
Change Management . . . . .	43
ALM Integration with Dimensions CM. . . . .	43
Sample Instances . . . . .	44
Database Accounts Used by Dimensions RM . . . . .	47
ICDBA Account . . . . .	47
Accounts Granted the Oracle RESOURCE Role . . . . .	47
Locking RM Oracle User Accounts . . . . .	48

Chapter 2

**Customizing Web Forms and Templates . . . . . 49**

- Customizing Web Forms . . . . . 50
  - Important Change to Web Forms Management . . . . . 50
  - Template Processing . . . . . 50
  - Template Layout . . . . . 50
  - Customizable Web Forms . . . . . 58
  - Allowable Tags . . . . . 59
- Defining Custom Styles for Exported Documents . . . . . 61
- Creating Templates to Export Requirements . . . . . 63
- Defining Headers and Footers for Exported Documents . . . . . 65
  - Creating a General Header and Footer File . . . . . 65
  - Creating a Template Header and Footer File . . . . . 66
- Exporting a Document with File Attachments from a Separate Server . . . 67
- Customizing RM Browser Menus and Title Bars . . . . . 68
  - Editing the Top Menu . . . . . 68
  - Editing the Action Pane of a View . . . . . 70
- Changing the Default Settings of the RM Browser Text Editor . . . . . 73
- Customizing the Editable Grid . . . . . 73
- Configuring the Expansion and Collapse of RM Browser Sections . . . . . 74
- Creating Custom Login Alert Pages for RM Browser . . . . . 74
- Customizing Headers and Footers of RM Browser Interface . . . . . 75
- Dashboard Export . . . . . 76
  - Using a Template . . . . . 76
  - Configuration . . . . . 77
  - Command Line Parameters . . . . . 78

Chapter 3

**Agile . . . . . 79**

- Creating Classes . . . . . 80
- Using Custom Classes . . . . . 80
  - Epics Class . . . . . 81
  - Features Class . . . . . 82
  - Products Class . . . . . 83
  - Releases Class . . . . . 84
  - Sprints Class . . . . . 86
  - Stories Class . . . . . 88
  - Tasks Class . . . . . 91
- Creating Relationships . . . . . 93
- Enabling Agile . . . . . 94
- Products and Subcategories . . . . . 94

Chapter 4

**Special Functions in Dimensions RM. . . . . 95**

- About Special Functions . . . . . 96
- NLP Complexity Analysis - Implementation . . . . . 96
- NLP Similarity Analysis - Implementation . . . . . 96
- Configuration for Branching and Merging . . . . . 97
- Defining the Document Class . . . . . 98
- Defining the Glossary Class . . . . . 99
- Risk Management . . . . . 99

	GitHub Integration . . . . .	102
	Chatbot Integration . . . . .	103
	Chatbot Installation . . . . .	103
	Docker Image Installation . . . . .	104
	Configuring the Chatbot . . . . .	105
	Jira Integration . . . . .	105
	IP Restrictions for Groups . . . . .	107
	Retrieving Group Infos . . . . .	107
	Enabling IP Restrictions . . . . .	108
	Disabling IP Restrictions . . . . .	109
	Restricting Groups by IP Addresses . . . . .	110
	Retrieving IP Addresses of Logged In Users . . . . .	111
	SSO and CAC Configuration . . . . .	111
	Configuring SSL Certificates . . . . .	112
	Configuring SSO with AD FS . . . . .	115
	Registry Keys and Configuration Files on the RM Server . . . . .	120
	Registry Keys and Configuration Files on the Fat Client . . . . .	123
	Troubleshooting . . . . .	124
	Redirecting Internal Web Service and REST Service Calls . . . . .	125
<i>Chapter 5</i>	<b>Test Management . . . . .</b>	<b>127</b>
	Test Management . . . . .	128
<i>Chapter 6</i>	<b>Logging . . . . .</b>	<b>131</b>
	Log Files . . . . .	132
	Logging Configuration File log4cpp.conf . . . . .	132
	Logging Configuration File log4net.config . . . . .	133
	Log Levels . . . . .	134
	Logging with RM Import . . . . .	135
	Logging Administrative Activities . . . . .	135
	About Administrative Logging . . . . .	135
	Actions for which Data Is Recorded . . . . .	136
	Archive Operations under Oracle . . . . .	140
	Remove Operations . . . . .	141
	Show Operations . . . . .	142
<i>Chapter 7</i>	<b>Application Lifecycle Framework (ALF) . . . . .</b>	<b>145</b>
	Overview . . . . .	146
	Architecture . . . . .	146
	Emitting ALF Events . . . . .	147
	Trigger Points . . . . .	148
	Event Definition . . . . .	149
	Event Emitter . . . . .	149
	Event Emitter Service . . . . .	149
	Dimensions RM Web Services . . . . .	149
	Enabling an Instance for ALF . . . . .	150
	Configuring the ALF Emitter Service . . . . .	151
	Usage . . . . .	151

Options . . . . .	152
Using Encrypted Passwords . . . . .	152
Installation . . . . .	153
Using SSL Authentication with ALF . . . . .	153
Logging . . . . .	155
Troubleshooting . . . . .	155
ALF Event Emitter Service Fails on Startup . . . . .	155

Chapter 8

<b>RM Manage . . . . .</b>	<b>157</b>
RM Manage Overview . . . . .	158
Configuring Workspace Options . . . . .	158
RM Home Directory . . . . .	158
Oracle Users Must Set ORACLE_HOME . . . . .	159
Setting the License Server . . . . .	159
The Location of the Database Password File . . . . .	160
Functions Available from RM Manage . . . . .	161
Creating the ICDBA Account . . . . .	161
Oracle Tablespace . . . . .	162
Managing Instances . . . . .	164
Creating an Instance with Oracle Databases . . . . .	164
Using Advanced Options When Creating a New Instance with Oracle Databases	172
Creating a New Instance with MS SQL Server Databases . . . . .	173
Creating a New Instance with PostgreSQL Databases . . . . .	175
Changing the Instance Password . . . . .	181
Updating the Instance Password . . . . .	182
Dimensions RM Backup . . . . .	182
Restoring an Instance Account from a Backup . . . . .	189
Backing Up Instances from the Command Line . . . . .	196
Converting Database and Instances . . . . .	201
Deleting an Instance Account . . . . .	201
Defining the Instance Schema . . . . .	202
Backing Up an Instance Schema . . . . .	202
Restoring an Instance Schema from a Backup . . . . .	203
Placing an Instance Account Online . . . . .	204
Placing an Instance Account Offline . . . . .	204
Installing Instance Tables . . . . .	204
Dropping Instance Tables . . . . .	205
Recreating Database Procedures . . . . .	205
Recreating Database Indexes . . . . .	205
Recreating Database Resources . . . . .	205
Setting Link Options for Baselines . . . . .	206
Managing Users and Groups . . . . .	206
Administering Users . . . . .	206
Administering Groups . . . . .	214
Assigning Users to Groups . . . . .	216
Group Security . . . . .	218
Deleting a User from an Instance . . . . .	223

Managing Security . . . . .	223
Default Access . . . . .	224
Database Administrator Accounts . . . . .	225
Changing an Instance Administrator Password . . . . .	231
Order of Precedence . . . . .	231
Valid Transactions . . . . .	232
Database Password Encryption . . . . .	235
Managing Databases . . . . .	235
Logging onto a Database . . . . .	236
Logging on as a Different User . . . . .	236
Converting a Database or Instance . . . . .	236
Administering Tablespaces . . . . .	237
Configuring E-Mail Notification. . . . .	240
Database Tab . . . . .	241
Mail Server Tab. . . . .	242
Control Tab . . . . .	243
Log Tab . . . . .	245
Notifications Tab . . . . .	245
General Tab . . . . .	246
Login Sources . . . . .	246
Specifying Login Sources in RM Manage. . . . .	247
Creating RM Users Automatically. . . . .	248
Changing the SSO Provider Host Name . . . . .	250
Fully Disabling SSO . . . . .	251
Specifying an LDAP Server . . . . .	252
Specifying the LDAP Configuration. . . . .	252
Configuring LDAP to Use SSL . . . . .	256
Using Two-Factor Authentication For Logins . . . . .	258
Setting Up Password Security . . . . .	258
Setting Password Rules . . . . .	259
ALM Integration Between Dimensions CM and Dimensions RM. . . . .	261
Logging In to a Dimensions CM Server. . . . .	261
Associating Dimensions RM Instances to Dimensions CM Products. . . . .	261
Associating Dimensions RM Baselines or Collections to Dimensions CM Projects/Streams. . . . .	261
Command Line Parameters . . . . .	261
Using RM Manage within the Amazon Cloud . . . . .	262
RM Manage Toolbars . . . . .	263
<b>Chapter 9</b>	
<b>Class Definition . . . . .</b>	<b>265</b>
Overview . . . . .	266
Defining the Instance Schema . . . . .	266
Class Definition Tasks . . . . .	266
Modeling Instances from Project Information . . . . .	267
Class Definition . . . . .	268
Class Attributes. . . . .	268
User Access to Classes. . . . .	269
Relationships Between Classes . . . . .	269

Relationship Rules . . . . .	269
Process Documentation Phase . . . . .	269
Attributes for Specific Classes . . . . .	270
Starting Class Definition . . . . .	270
Working with the Class Definition Diagram . . . . .	271
Editing the Instance Header and Footer . . . . .	271
Aligning Components . . . . .	271
Canvas Grid . . . . .	272
Centering the Diagram . . . . .	272
Changing the Canvas Size . . . . .	272
Finding a Class or Relationship . . . . .	273
Nudging Objects . . . . .	274
Ordering Objects . . . . .	274
Panning the Diagram . . . . .	274
Selecting Objects . . . . .	275
Zooming the Diagram . . . . .	275
Attributes . . . . .	275
Attribute Types . . . . .	276
Adding an Attribute . . . . .	295
Defining an Attribute . . . . .	295
Retiring an Attribute . . . . .	298
Deleting an Attribute . . . . .	298
Classes . . . . .	298
Adding a New Class . . . . .	299
Changing Display Properties for a Class . . . . .	300
Changing a Class Image . . . . .	300
Copying a Class . . . . .	301
Creating a Class Type from a Class . . . . .	301
Deleting a Class . . . . .	301
Purging Class Data . . . . .	302
Renaming a Class . . . . .	302
Defining a Class . . . . .	302
Specifying Attributes . . . . .	304
Specifying a Description . . . . .	305
Specifying Security . . . . .	305
Specifying Equal Control Width on Forms . . . . .	305
Relationships . . . . .	306
Adding a New Relationship . . . . .	306
Changing the Display Properties for a Relationship . . . . .	306
Deleting a Relationship . . . . .	307
Editing Vertices . . . . .	308
Purging Relationship Data . . . . .	308
Renaming a Relationship . . . . .	309
Reversing a Relationship . . . . .	309
Defining a Relationship . . . . .	309
Specifying Attributes . . . . .	310
Specifying a Description . . . . .	310
Specifying Constraints . . . . .	311

Specifying Security . . . . .	316
Class Types . . . . .	316
Manage Class Types . . . . .	317
Adding a New Class Type . . . . .	317
Deleting a Class Type . . . . .	318
Editing a Class Type Definition . . . . .	318
Specifying Attributes . . . . .	318
Changing the Class Definition Bitmap . . . . .	318
Changing the Class Icon . . . . .	319
Changing the Label Properties for Class Types . . . . .	320
Security . . . . .	320
Granting Group Access . . . . .	320
Valid Actions . . . . .	321
Saving the Instance Schema . . . . .	323
Reloading the Instance Schema . . . . .	324
Releasing the Instance Schema Lock . . . . .	324
Deploying the Instance Schema . . . . .	324
Deploying the Schema Locally . . . . .	325
Deploying the Schema Across the Network . . . . .	325
Printing the Instance Schema Diagram . . . . .	326
Printing the Instance Schema Definitions . . . . .	326
Implementing Suspect Links . . . . .	327
Defining the Date Format . . . . .	327
Date Format Elements . . . . .	328
Date Format Element Suffixes . . . . .	330
Capitalization of Date Format Elements . . . . .	330
RRRR Date Format Elements . . . . .	330
Punctuation and Character Literals in Date Format Models . . . . .	331
Workflows . . . . .	331
Workflow Elements . . . . .	332
Creating or Editing a Workflow . . . . .	332
Copying a Workflow to another Class . . . . .	344
Deleting a Workflow . . . . .	345
Using Containers with Workflows . . . . .	346
Creating Product and Project Classes . . . . .	347
Creating Product and Project Classes for Branching . . . . .	347
Creating Product or Project Classes without Branching . . . . .	347
Supporting Comments . . . . .	348
Overview . . . . .	348
Adding the Comment Class and Relationships . . . . .	349
<b>Chapter 10</b>	
<b>Configuring Tomcat . . . . .</b>	<b>351</b>
Working with Secure Socket Layers . . . . .	352
Configuration Overview . . . . .	352
Importing the Dimensions RM Server Certificate . . . . .	352
Updating the Dimensions RM Server Certificate . . . . .	357
Importing Certificates on the Client . . . . .	366
Configuring Secure Cookies . . . . .	367

	Configuring HTTP Strict Transport Security and Anti-Clickjacking . . . . .	369
	Restricting Server.xml User Access . . . . .	369
	Configuring the Tomcat Service . . . . .	370
	Preparing Configuration . . . . .	370
	Removing the Certificate Update Menu . . . . .	370
<b>Chapter 11</b>	<b>RM Import . . . . .</b>	<b>373</b>
	RM Import Overview . . . . .	374
	Logging in to RM Import . . . . .	375
	Command Line RM Import . . . . .	377
	Input File Format Dialog . . . . .	377
	Word Import . . . . .	378
	Date Import Formats . . . . .	379
	Preview Dialog . . . . .	380
	Draft Requirements Document Import . . . . .	383
	Excel Import . . . . .	383
	Selecting an Excel File . . . . .	384
	Mapping Excel Columns to RM Attributes . . . . .	384
	Configuring Import Rules . . . . .	386
	Configuring Document Settings . . . . .	387
	Importing . . . . .	388
	Configuring RM Import . . . . .	388
	Configuring the Security Protocol . . . . .	388
<b>Chapter 12</b>	<b>WIRIS Editor . . . . .</b>	<b>391</b>
	Overview . . . . .	392
	Installing the WIRIS Editor . . . . .	392
	Configuring the WIRIS Editor . . . . .	392
	Configuring Dimensions RM for the WIRIS Editor . . . . .	395
	Configuring the HTML Editor . . . . .	395
	Configuring the Inline HTML Editor . . . . .	396
	Configuring the Editable Grid . . . . .	397
	Restart Dimensions RM Services . . . . .	397
<b>Chapter 13</b>	<b>RM Import Designer . . . . .</b>	<b>399</b>
	RM Import Designer Overview . . . . .	400
	Logging in to RM Import Designer . . . . .	401
	Commands . . . . .	403
	Opening an Existing Template . . . . .	403
	Creating a New Template . . . . .	404
	Saving a Template . . . . .	404
	Saving a Template with Another Name . . . . .	404
	Deleting a Template . . . . .	405
	General Tab . . . . .	406
	Chapter Rules Tab . . . . .	407
	Requirement Rules Tab . . . . .	408
	Table Option . . . . .	408
	Section Option . . . . .	409

	Keyword Option . . . . .	410
	Class Rules Tab . . . . .	412
	Class Information . . . . .	412
	Attribute Information . . . . .	415
	Preview Tab . . . . .	424
	Word Regular Expressions . . . . .	425
	Example Word Regular Expressions . . . . .	427
	Limitations . . . . .	427
	Examples . . . . .	428
<i>Appendix A</i>	<b>Handling Certificates . . . . .</b>	<b>429</b>
	Importing a PFX Certificate into Microsoft IIS . . . . .	430
	Importing a PFX Certificate into Windows . . . . .	430
	Exporting Certificates . . . . .	432
	Exporting Certificates to CER Format from the Management Console . . . . .	432
	Exporting Certificates to CER Format from IIS . . . . .	433
	Exporting Certificates to PFX Format from the Management Console . . . . .	434
	Exporting Certificates to PFX Format from IIS . . . . .	435
	Exporting a Certificate from the STS Server from the Command Prompt . . . . .	437
	Exporting the STS Certificate from SBM Configurator . . . . .	438
	Listing all Certificates in a Keystore . . . . .	439
	Retrieving the Alias from a PFX File . . . . .	439
	Retrieving Root CA and Intermediate CA Certificate Files . . . . .	440
	Importing Root and Intermediate CA into Local Certificate Store . . . . .	442
<i>Appendix B</i>	<b>Database Security . . . . .</b>	<b>445</b>
	Overview . . . . .	446
	Oracle Database Security . . . . .	446
	Shall I use Transport Encryption or Native Network Encryption? . . . . .	446
	Transport Encryption with Oracle . . . . .	446
	Native Network Encryption with Oracle . . . . .	452
	Transparent Data Encryption with Oracle . . . . .	453
	MS SQL Server Database Security . . . . .	457
	Transparent Data Encryption with MS SQL Server . . . . .	460
	PostgreSQL Database Security . . . . .	463
	Transport Encryption with PostgreSQL . . . . .	463
	Transparent Data Encryption with PostgreSQL . . . . .	463
<i>Appendix C</i>	<b>Troubleshooting . . . . .</b>	<b>465</b>
	Resolving "Password May be Incorrect in Security File or Security File May Not be Found" Error . . . . .	466
	Using CAC and Unable to Perform RM Browser User Management . . . . .	467
	Unable to create ICDBA Account or RM Instance . . . . .	467
	RM Browser hangs when Exporting Documents . . . . .	467
	Windows Server is not prepared for Microsoft Office . . . . .	467
	Adobe Reader is installed on Windows Server . . . . .	468
	A Server Upgrade has Broken Office . . . . .	468
	Exporting Documents creates DOC Files . . . . .	468

	Export of Requirements creates XLS Files . . . . .	468
	Unable to Export Dashboards . . . . .	468
	Word cannot open Documents. . . . .	468
	Unable to Save Query Results or Export Documents. . . . .	469
	RM Manage crashes when connecting to Dimensions CM. . . . .	469
	Unable to Re-login in Firefox . . . . .	469
	Addressing Database Performance . . . . .	470
	For all Supported Databases. . . . .	470
	MS SQL Server Performance Issues. . . . .	470
<i>Appendix D</i>	<b>RM Import Designer Examples . . . . .</b>	<b>471</b>
	Overview . . . . .	472
	Begin and End Keyword . . . . .	472
	Entire Table with a Keyword is the Requirement . . . . .	474
	Table Option with Every Row. . . . .	475
	Section Option with Keywords . . . . .	477
	Heading Styles . . . . .	479
	Capturing Title and Description with No Title Rule . . . . .	480
	Capturing Title and Description with Title Rule. . . . .	482
<i>Appendix E</i>	<b>URL Syntax . . . . .</b>	<b>485</b>
	How to Manually Specify a URL for URL Addressable Views . . . . .	486
	URL to a Document . . . . .	486
	URL to a Chapter of a Document. . . . .	486
	URL to a Snapshot of a Document. . . . .	486
	URL to Export a Document . . . . .	486
	URL to a Collection . . . . .	487
	URL to a Specific Version of a Requirement . . . . .	487
	URL to compare History Versions of a Requirement . . . . .	488
	URL to the Current Version of a Requirement . . . . .	488
<i>Appendix F</i>	<b>Word Document Post Processing . . . . .</b>	<b>491</b>
	Post Processing Overview . . . . .	492
	About Word Document Post Processor . . . . .	492
	Settings . . . . .	493
	Enabling Word Document Post Processor . . . . .	498
	Disabling Word Document Post Processor. . . . .	499
	About Custom Word Document Post Processor . . . . .	499
	Enabling Custom Word Document Post Processor . . . . .	499
<i>Appendix G</i>	<b>Word Import Pre-Processing . . . . .</b>	<b>501</b>
	Overview . . . . .	502
	Settings . . . . .	502
	Selector Settings. . . . .	506
<i>Appendix H</i>	<b>Automatic Termination of MS Word . . . . .</b>	<b>511</b>
	Overview . . . . .	512
	Settings . . . . .	512

---

<i>Appendix I</i>	<b>Configuration and Usage of ServiceHelper . . . . .</b>	<b>513</b>
	Overview . . . . .	514
	Settings . . . . .	514
	Usage. . . . .	518
	Retrieving Dimensions RM Configuration . . . . .	518
	Getting a List of RM Services . . . . .	518
	Getting System Information . . . . .	519
	Importing Certificates into a System Keystore . . . . .	519
	Restarting RM Pool Manager . . . . .	520
	Restarting Tomcat. . . . .	520
	Restarting a Service . . . . .	521
	Starting a Service . . . . .	521
	Stopping a Service . . . . .	521
	Splitting a PFX Certificate. . . . .	522
<i>Appendix J</i>	<b>Azure Active Directory . . . . .</b>	<b>523</b>
	Microsoft Azure . . . . .	524
	Registering Dimensions RM as Azure Application . . . . .	524
	Retrieving Configuration Data from Azure AD . . . . .	525
	Azure SAML2 Authentication . . . . .	528
<i>Appendix K</i>	<b>Configuring Windows SSO . . . . .</b>	<b>533</b>
	About Windows SSO. . . . .	534
	Configuring Windows SSO. . . . .	534
	<b>Index. . . . .</b>	<b>535</b>



# Preface

---

## Objective

The purpose of this manual is to describe how to configure, manage, and administer Dimensions RM instances, users, and groups. Dimensions RM is 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 manual supersedes earlier editions of this manual.

## Audience

This manual is intended for Dimensions RM administrators responsible for creating and managing instances, users, and groups.

## 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.
<b>bold</b>	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.
<i>monospaced italics</i>	Indicates names that are placeholders for values you specify; for example, <i>filename</i> .
<b>monospace bold</b>	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

Open Text 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 Open Text Support at the following URL and follow the instructions:

<http://supportline.microfocus.com>

Language-specific technical support is available during local business hours; after hours technical support is provided in English.

The Open Text 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 Open Text products.

## **License and Copyright Information for Third-Party Software**

For license and copyright information of third-party software included in this release, check the file `Third_Party_Licenses.txt`, which can be found in the Dimensions RM installation directory, e.g. `C:\Program Files\Open Text\Dimensions 25.2\RM`.



# Chapter 1

---

## Dimensions RM Overview

The Role of the System Administrator	20
The Role of Requirements Management	20
Dimensions RM Data Structure	23
Dimensions RM Basics	24
Sample Instances	44
Database Accounts Used by Dimensions RM	47

## The Role of the System Administrator

Dimensions RM is the Open Text Software solution for requirements management, delivering an enterprise-wide solution based on either Oracle® RDBMS, Microsoft SQL Server, or PostgreSQL.

This guide answers questions relating to the installation, configuration and management of the Dimensions RM environment. These are tasks implemented by the individuals assigned the role of **System Administrator**, the only users with access to the administration tool: **RM Manage**.

The **System Administrator** may work with various project teams to create new database instances, define the schema that best suits the needs of the organization, and then make that schema available to the Instance Manager for continued definition and maintenance.

The **Instance Administration** group is assigned permissions to all Actions necessary to the management of the instance, for example, modifying the Schema Definition, adding users to the instance and defining their access, defining and managing categories, notifications and the basic settings that define the working world for instance users.

## The Role of Requirements Management

Requirements management is the process by which an engineering project records and maintains the official, binding description of what it plans to achieve. With Dimensions RM teams are also able to maintain a system of record for what has been achieved.

The requirements management process includes the following activities:

- Requirement development.
- Reporting and traceability.
- Change management.
- Communication

### Requirement Development

One of the first steps in every project is the specification of requirements. Tracking these requirements across different organizations and understanding the impact that various requirements have on cost, schedule, and time-to-market can have a dramatic effect on project success.

Dimensions RM stores requirements in a database. The requirements for a project can come from various sources, such as customers, management, Marketing, Quality Assurance (QA), Support, and field personnel. The requirements can be entered directly into Dimensions RM, or imported from a Microsoft® Word document, plain text document, excel or XML. Documents can be synchronized with the database as requirements evolve.

Requirements can also be imported from other tools, such as Open Text Solution Business Manager or DevOps. For more information about the integration of Dimensions RM with these products, see the relevant manual in the complete Dimensions RM doc set.

## Reporting and Traceability

With traceability, users can evaluate the effects of changes in requirements and identify potential problems. Traceability involves making explicit links between requirements and other entities.

For example, suppose you link marketing requirements to test cases. You then run a report on this relationship. The report shows marketing requirements on the left side of the report, and any associated test cases on the right side of the report. This format allows you to easily determine which marketing requirements lack associated test cases. Another type of traceability report you can create in RM Browser shows the requirements in the relationship in a tree-like structure.

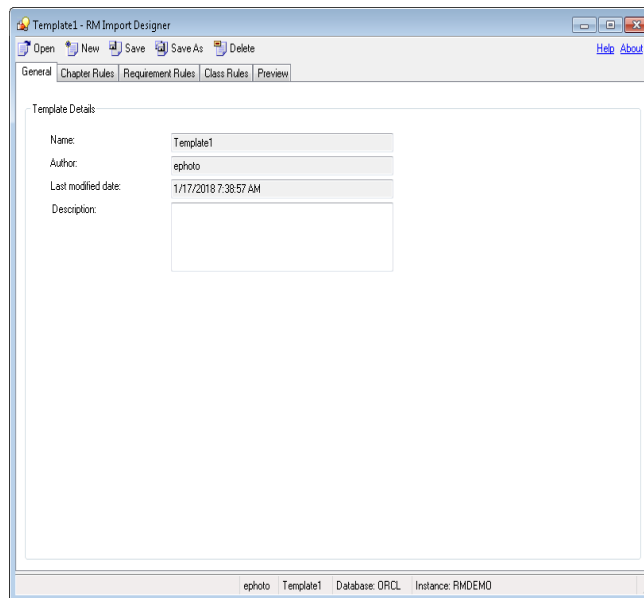
## Change Management

Requirements change over time. The change management activity within a requirements management process involves preventing unauthorized changes, gathering the information necessary to make informed decisions about which changes to allow, and making those changes in a systematic way.

In Dimensions RM, you can submit a change request against a specific requirement. If a Dimensions RM Tools

The following sections briefly describe the Dimensions RM tools. The Dimensions RM tools are the various interfaces you use to perform specific tasks.

## RM Import Designer

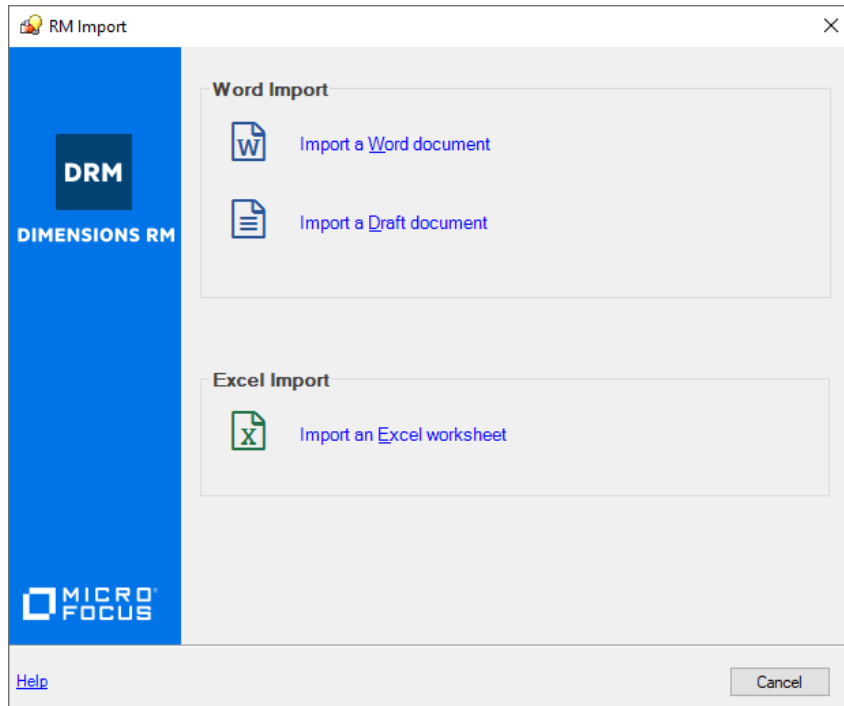


**Figure 1-1. RM Import Designer**

RM Import Designer allows power users to design templates that may be selected when importing Word documents using RM Import. Templates define how to identify classes, attributes, chapters, requirements, and categories. Templates can be saved to the database for future use. Power users who develop templates must be knowledgeable about class types and the structure of the Word documents that will be imported. For

detailed information about using RM Import Designer, see ["RM Import Designer"](#) on page 399.

## RM Import

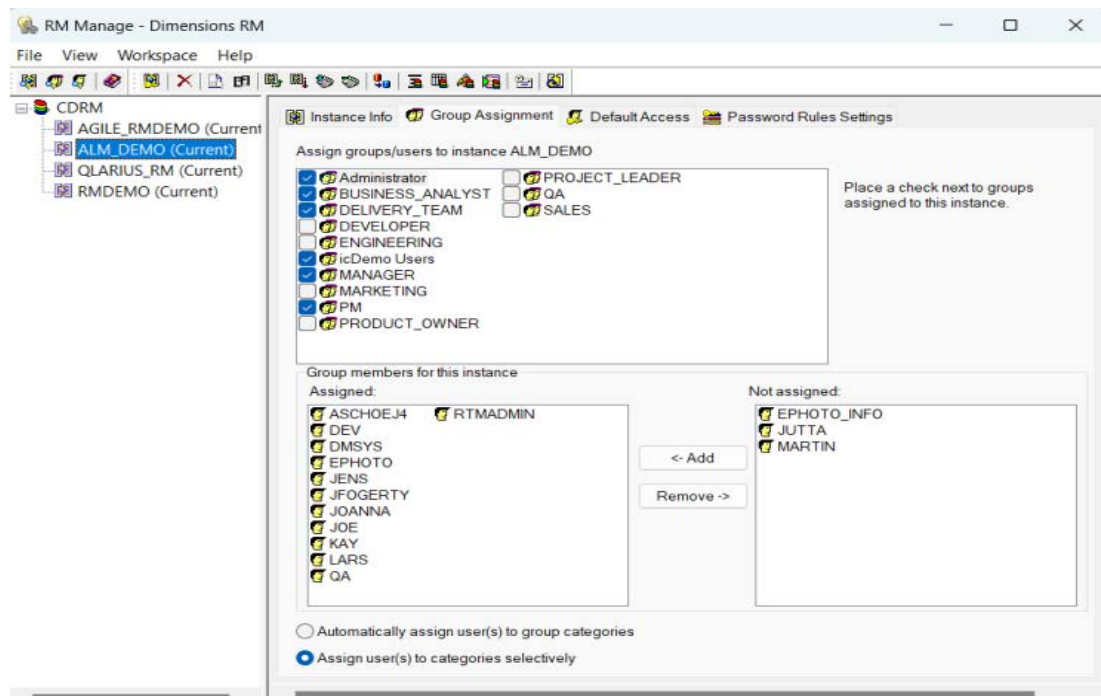


**Figure 1-2. RM Import**

RM Import allows users to preview a Word document as a draft document, change the description of chapters, reorganize the chapters, change the values of attributes, and move attributes between chapters. When satisfied with the draft, users can import the document into Dimensions RM as a document. For detailed information about using RM Import, see chapter ["RM Import"](#) on page 373.

It is also possible to import Word documents using RM Browser. Many Word documents can be imported using the RM Browser. We recommend reviewing the Chapter, "Importing Requirements" in the *Dimensions RM Browser User's Guide*.

## RM Manage



**Figure 1-3. Group Assignments for Instance ALM\_DEMO**

RM Manage allows **System Administrators** to create and configure the database, create instances and perform the general care and feeding of server and database. For detailed information see Chapter "RM Manage" on page 157.

## Class Definition

The database is designed to hold one or more Instances. The *Instance* is the main focus of activity in RM, all requirements and associated data are stored within its confines. A single instance may be used to manage all requirements associated with a set of products or components, or, depending on interrelationships, multiple instances may be used.

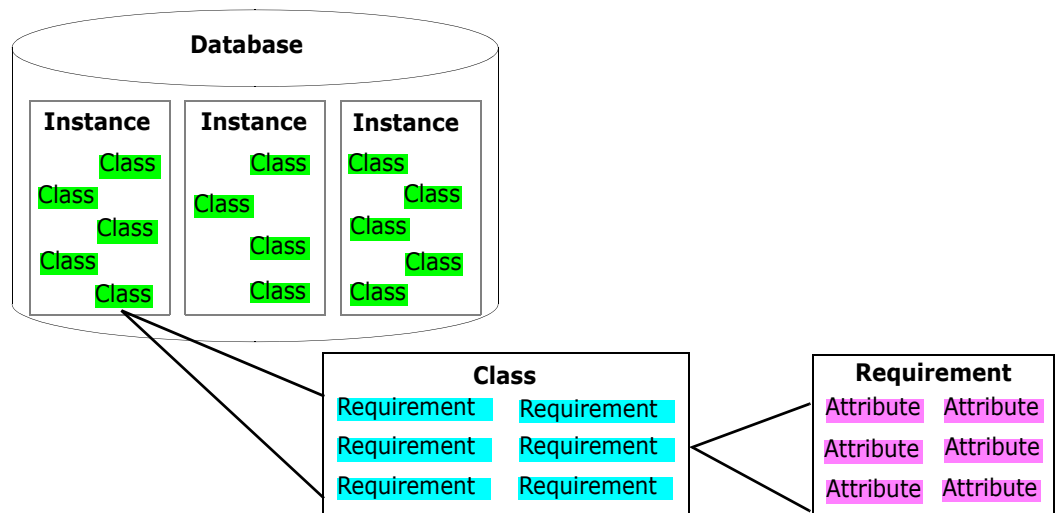
Class Definition (referred to as Schema Definition in the RM Browser) allows **System Administrators** to create the Instance and, perhaps, initially populate it by defining classes, or deploying existing classes from existing Instances.

For detailed information about the initial definition of classes, relationships, and attributes, see "Class Definition" on page 265.

Once created, the process of defining or modifying classes, relationships, attributes, and security may be accomplished in the browser by the Instance Administrators. see the section "Editing the Instance Schema" in the *Dimensions RM Browser User's Guide*.

## Dimensions RM Data Structure

The following diagram illustrates the Dimensions RM data structure.



**Figure 1-4. Dimensions RM Data Structure**

The resources in the data structure are explained in detail later in this chapter. For purposes of illustration, however, consider the example in the following table.

We refer to the objects stored within this class as “Requirements” however, they are objects stored with attributes and may be associated with design, test, release, or any aspect of the application lifecycle.

Resource	Value
Instance 1	RELEASE1
Class	Customer_Requirements
Requirement	CUST_000007
Attributes	Rqmt ID = <i>CUST_000007</i> Document ID = <i>Customer Requirements</i> Rollout Plan = <i>First Release</i> Priority = <i>Priority 1</i> Object ID = <i>7</i> Paragraph ID = <i>3.1.6</i> Paragraph Title = <i>Configuration</i> Current Status = <i>Current</i> Text = <i>All preferences shall be remembered between invocations.</i>

## Dimensions RM Basics

This section provides an overview of basic Dimensions RM concepts.

### Users and Groups

Users and groups are defined within each Dimensions RM database and are associated with specific instances in the database.

Each Dimensions RM user has a password-protected account within Dimensions RM that identifies the user. The account stores information such as the user's first and last names, and e-mail address. The user name is associated with all modifications made to the instance.



**NOTE** Dimensions RM user accounts are distinct from operating system user accounts.

Dimensions RM users are organized into groups that share access privileges. Individual users can be associated with any number of instances through their group memberships

Dimensions RM user groups usually match organizational groups or roles such as Managers, Developers, QA Engineers, and System Engineers, which can then be assigned to products or projects.

Each Dimensions RM instance supports an Administrator (Instance Administrator) group. Users assigned to this group may add users or groups to their assigned instance, as well as to modify their access.

## Instance Schemas

Each Dimensions RM instance has its own schema that defines the types of information to be managed in the instance. A schema contains a number of class and relationship definitions. Class definitions must be in place to create requirements, and relationship definitions must be in place to create links between requirements.

The instance schema does not have to be completely defined before useful work can be accomplished; teams may begin work with the classes and relationships that they will use immediately. As the instance evolves, other classes and relationships can be added and existing classes can be changed; this additional work may be accomplished by the Instance Administrator in the RM Browser tool.

Schemas are created in the Class Definition tool, accessible from RM Manage, or using Schema Definition from RM Browser. For an illustration of a class definition diagram, see ["Class Definition" on page 23](#). For information about using Class Definition, see Chapter ["Class Definition" on page 265](#).

## Classes and Requirements

Dimensions RM classes are used to define and control the information types to be managed within an instance. Typically, Dimensions RM classes correspond to the work products of the engineering lifecycle processes supported. Common examples of classes include requirements for Marketing, Customer Requests, Security, Software, Hardware, Test Cases, and Task lists.

Dimensions RM predefines many classes to be used as templates for class definitions. You can also build your own classes. In class definition diagrams, a class is represented by an icon.

A requirement is an instance of a class.

## Relationships and Links

Dimensions RM relationships define the associations between classes. For example, you can create a relationship between the `Customer_Requirement` and `Test_Cases` classes that enables you to link a test case to the customer requirements that it fulfills.

Relationships between classes enable the following functions:

- Generating reports containing data from multiple classes.
- Checking completeness of data.
- Building database subsets.
- Assessing impact analysis through traceability.

A *link* (for example, an association between a specific customer requirement and a specific test case) is an instance of a relationship. You can link two requirements together if a relationship between their corresponding classes is defined.

In class definition diagrams, a relationship is represented by an arrow connecting two classes. Relationships are directional, where a *primary* class points to a *secondary* class. This distinction is important when navigating and reporting on links between requirements. You can follow a link in either direction, but in many cases, you must know which class is primary and which class is secondary to create effective reports.



**NOTE** Words in relationship names must be connected with underscores.

## Attributes

Classes and relationships represent logical groupings of information. Each class definition and each relationship definition includes its name and its attributes. Attributes characterize the class or relationship in terms of its properties. For example, a `Customer_Requirements` class could have attributes for a title, a rationale, a textual statement of the requirement, and a priority.

Dimensions RM supplies a core set of *implicit* attributes for each class and relationship. Dimensions RM uses implicit attributes to maintain the integrity of instance information. Implicit attributes include intrinsic information such as the persistent unique identifiers (PUIDs), object IDs, and modification times. You cannot modify implicit attributes; however you can modify their display names.

You can create *user-defined* attributes for use in a specific class. Dimensions RM provides the following attribute types from which to create user-defined attributes:

Attribute Type	Description
Alphanumeric	Represents one line of alphanumeric text, such as the title of an acceptance test. It can be up to 1000 characters in length.
Date	Stores values that are based on user-defined date formats (for example, DDMMYY, YYYYMMDD, and so on). A date attribute, for example, could be used for dates in which test cases are performed.

Attribute Type	Description
File Attachment	Can hold one or multiple files that can be accessed through RM Browser. For example, you could add the file attachment attributes <i>Use Cases</i> , <i>Customer Letter</i> , and <i>Business Justification</i> to the Marketing Requirements class. Users can then use RM Browser to add, view, or download the file(s). File attachments can also be included as links in Word documents exported from Document View. The links are displayed as icons. You can double-click the icon in the exported document to open the associated file.
List	Provides a list of values from which users make a selection. For example, you could list <i>Pass</i> , <i>Fail</i> , and <i>Untested</i> as valid values for a list attribute named <code>test_result</code> .
Numeric	Holds numeric values, such as reference numbers. The numbers can include decimal points.
Text	Holds up to 64 KB of plain text or HTML text that can span more than one line. It is suitable for long descriptions, such as the description of an acceptance test. In RM Browser, when you click in or tab to a text attribute, an HTML editor opens. The HTML editor provides many common features of word processors.

When you create a user-defined attribute, you can also specify additional properties such as constraints on possible values, and whether an attribute value is mandatory. You can provide a default value to be used for a mandatory attribute when an actual value is not yet available.

## Security

Access rights are associated with each resource defined in a Dimensions RM database. Access rights determine if you can perform a task on a target resource.

The instance administrator uses the Class Definition tool to grant or deny access to resources defined in the instance schema. This includes all classes, relationships, attributes, and source documents. The list of valid transactions for each of these different resources varies. If the instance administrator does not grant or deny access to a specific resource in Class Definition, the default access defined in RM Manage for the resource category is used.

## Naming Conventions

Naming conventions are relevant for instances, classes, attributes, categories, relationships, Workflow transitions and Workflow states.



**NOTE** When using characters that are outside the regular ASCII charset (e.g. German Umlauts, or Chinese or Japanese characters), up to 4 bytes will be required to store one character. For example, the German ß character requires 2 bytes, while the Chinese character 口 uses 3 bytes. As the database (Oracle and SQL Server) use UTF-8 encoding, this means that the number of actual characters that can be used for a category name for example, depends on **which** characters are used. The sub-chapters that describe the naming conventions will deal with this by specifying the maximum number of characters.

### ***Naming Conventions for Instances***

**For instance names, the following naming conventions apply:**

- **Allowed characters:**
  - Letters A-Z, a-z
  - Numbers
  - Underscore (\_)
  - Hyphen (-)
- **Maximum length:** Up to 30 characters
- Instance name must not be one of the reserved words (see ["Reserved Words" on page 30](#)).
- Restrictions as specified for user names of your database.

### ***Naming Conventions for Class Names***

**For class names, the following naming conventions apply:**

- **Allowed characters:**
  - Letters A-Z, a-z
  - Unicode characters
  - Numbers
  - Underscore (\_)
  - Hyphen (-)
  - Ampersand (&)
  - Colon (:)
- **Maximum length:** Up to 1024 characters
- Class name must not be one of the reserved words (see ["Reserved Words" on page 30](#)).

### ***Naming Conventions for Attribute Display Names***

- **Allowed characters:**
  - Letters A-Z, a-z
  - Unicode characters
  - Numbers
  - Underscore (\_)
  - Hyphen (-)
  - Ampersand (&)
  - Colon (:)

- Space
- **Maximum length:** Up to 1024 characters
- Attribute display name must not be one of the reserved words (see ["Reserved Words" on page 30](#)).

### ***Naming Conventions for Attribute Names***

- **Allowed characters:**
  - Letters A-Z, a-z
  - Numbers
  - Underscore (\_)
  - Hyphen (-)
  - Ampersand (&)
  - Colon (:)
- **Maximum length:** Up to 1024 characters
- Attribute name must not start with **RTM\_**.
- Attribute name must not be one of the reserved words (see ["Reserved Words" on page 30](#)).

### ***Naming Conventions for Relationship Names***

- **Allowed characters:**
  - Letters A-Z, a-z
  - Unicode characters
  - Numbers
  - Underscore (\_)
  - Hyphen (-)
  - Ampersand (&)
  - Colon (:)
- **Maximum length:** Up to 1024 characters
- Relationship name must not be one of the reserved words (see ["Reserved Words" on page 30](#)).

### ***Naming Conventions for Workflow State Names***

- **Allowed characters:** All ASCII characters and Unicode characters
- **Maximum length:** Up to 1024 characters

### ***Naming Conventions for Workflow Transition Names***

- **Allowed characters:** All ASCII characters and Unicode characters
- **Maximum length: Up to 1024 characters**

### ***Reserved Words***

#### **A**

- ACCESS
- ADD
- ALL
- ALL
- ALTER
- AND
- ANY
- AS
- ASC
- AUDIT
- AVER
- AVERAGE

#### **B**

- BETWEEN
- BY

#### **C**

- CALC
- CALCULATE
- CHAR
- CHECK
- CLAR\_CONDITION
- CLASS\_NAME
- CLUSTER
- COLUMN
- COMPRESS
- CONNECT
- COUNT

- CREATE
- CURRENT

## **D**

- DATALESS\_TAG\_COLUMN
- DATE
- DATE\_CREATED
- DATE\_LAST\_MODIFIED
- DBA
- DECIMAL
- DEFAULT
- DELETE
- DESC
- DISTINCT
- DROP
- DTP\_TEXT

## **E**

- ELSE
- EXCLUSIVE
- EXISTS
- EXPAND

## **F**

- FILE
- FIRST
- FLOAT
- FOCUS
- FOR
- FOURTH
- FROM

## **G**

- GEN\_KEY\_COLUMN
- GRANT
- GRAPHIC
- GROUP

## H

- HAVING
- HAVING\_CLARIFICATION\_TEXT
- HAVING\_NO\_CLARIFICATION\_TEXT
- HAVING\_NO\_QUERY\_TEXT
- HAVING\_QUERY\_TEXT

## I

- IDENTIFIED
- IF
- IMMEDIATE
- IMMEDIATE\_XREF
- IN
- INCREMENT
- INDEX
- INITIAL
- INITIALIZED
- INSERT
- INTEGER
- INTERSECT
- INTO
- IS

## K

- KEY
- KEYWORD\_COLUMN
- KEY\_LIST\_CONDITION

## L

- LEVEL
- LIKE
- LINKS\_IN
- LOCK
- LONG
- LOWEST\_LEVEL\_REQUIREMENT\_CONDITION

## M

- MATH\_OP
- MATH\_TAG
- MAX
- MAXEXTENTS
- MAXIMISE
- MAXIMUM
- MIN
- MINIMISE
- MINIMUM
- MINUS
- MODE
- MODIFY

## **N**

- NOAUDIT
- NOCOMPRESS
- NORM
- NORMALISE
- NORMALIZE
- NOT
- NOT\_LOWEST\_LEVEL\_REQUIREMENT\_CONDITION
- NOT\_PRIMARY\_IN
- NOT\_PRIMARY\_IN\_CONDITION
- NOT\_SECONDARY\_IN
- NOT\_SECONDARY\_IN\_CONDITION
- NOT\_SOURCE\_REQUIREMENT\_CONDITION
- NOWAIT
- NULL
- NUMBER

## **O**

- OF
- OFFLINE
- ON
- ONLINE
- OPTION

- OR
- ORDER
- ORDER\_COLUMN

## **P**

- PCTFREE
- POP
- POPULATED
- PRIMARY
- PRIMARY\_HISTORY
- PRIMARY\_IN
- PRIMARY\_IN\_CONDITION
- PRIMARY\_IN\_RELATIONSHIP
- PRIOR
- PRIVILEGES
- PUBLIC

## **Q**

- QUERY\_CONDITION

## **R**

- RAW
- RELATIONSHIP\_COLUMN
- RENAME
- REPLACE
- RESOURCE
- REVOKE
- ROW
- ROWID
- ROWNUM
- ROWS

## **S**

- SECOND
- SECONDARY
- SECONDARY\_HISTORY
- SECONDARY\_IN

- SECONDARY\_IN\_CONDITION
- SECONDARY\_IN\_RELATIONSHIP
- SELECT
- SESSION
- SET
- SHARE
- SIZE
- SMALLINT
- SOURCE
- SOURCE\_DOC
- SOURCE\_DOC\_TREE
- SOURCE\_REQUIREMENT\_CONDITION
- SOURCE\_XREF
- START
- SUCCESSFUL
- SYNONYM
- SYSDATE

## T

- TABLE
- THEN
- THIRD
- TO
- TOTAL
- TRIGGER
- TypeNameHere

## U

- UID
- UNION
- UNIQUE
- UPDATE
- USER
- USING

## V

- VALIDATE

- VALUES
- VARCHAR
- VARGRAPHIC
- VIEW

## W

- WHENEVER
- WHERE
- WITH
- WITHOUT\_CLAR\_CONDITION
- WITHOUT\_QUERY\_CONDITION
- WITH\_CLAR\_CONDITION
- WITH\_QUERY\_CONDITION

## X

- XREF

## Categories

Categories are represented by a hierarchical structure inside each Dimensions RM instance, with sub-categories supported. Categories work like folders on a file system, with "favorites" selected such that an individual user can set and easily access defaults. For further information about categories, see chapter *"Managing Categories"* in the *Dimensions RM Browser User's Guide*.

## Requirement Creation

You can use the following methods to create requirements:

- Capture requirements from documents

You can capture requirements from Microsoft Word documents using RM Import Designer and RM Import, and with Microsoft Word Tables using RM Browser. Excel files saved as tab separated text, comma separated or semi-colon separated files can also be imported using the browser.
- Enter and modify requirements also using RM Browser.
- Import requirements from another tool such as Open Text Solution Business Manager (formerly known as Serena<sup>®</sup> Business Manager, Serena<sup>®</sup> Business Mashups and TeamTrack), IBM<sup>®</sup> Rational<sup>®</sup> Software Modeler, HP Quality Center, Microsoft<sup>®</sup> Project, and Microsoft<sup>®</sup> Excel<sup>®</sup>.

## Requirement Evolution

As you evolve requirements within Dimensions RM, their history is retained so that you can trace the evolution of a requirement from its creation through to the current version. There is an implicit parent-child link between successive versions of a requirement.

### **Audit Trail**

As you evolve requirements within your project, Dimensions RM retains the various versions of your requirements. This historical trace, known as the *audit trail*, allows you to reconstruct requirement evolution when needed (for example, to evaluate progress over time). At each stage of the evolution, you can record a rationale for changes, thus retaining project knowledge as well as the physical changes.

### **Current Status**

A special implicit attribute, Current Status, identifies the state of the requirement. The Current Status values are described in the following table.

Current Status	Description
Current	The requirement is the most recent or current version.
Replaced	The requirement has been replaced by a newer version.
Proposed	A change request has been made to either change the current requirement or create a new requirement.
Accepted	A change request was accepted.
Rejected	A change request was rejected.
Deleted	The Current Status of the requirement is changed to Deleted, but the requirement remains in the instance. The prior version of the requirement, if any, is given a current status of Current.

### **Operations on Requirements**

There are two commands for saving changes you made to a requirement:

- **Update**—The Update command changes the content of the requirement as you specify, leaving all other attributes, including Current Status, intact. Update is often best reserved for minor changes such as correcting typographical errors. Because the requirement is not versioned with the Update command, it is highly recommended that only instance administrators have permission to perform updates.
- **Replace**—The Replace command creates a new version of the requirement with the changes you made. With Replace, the Current Status of the original requirement is changed from Current to Replaced, a parent-child link is created from the original requirement to the new requirement, and the Current Status of the new requirement is set to Current.
- **Copy**—The Copy command creates a new requirement with the same attribute values as another requirement. You specify the attributes to be copied in Class Definition. For more information, see ["Attributes" on page 275](#).

There are three commands that allow you to correct mistakes or undo changes you made:

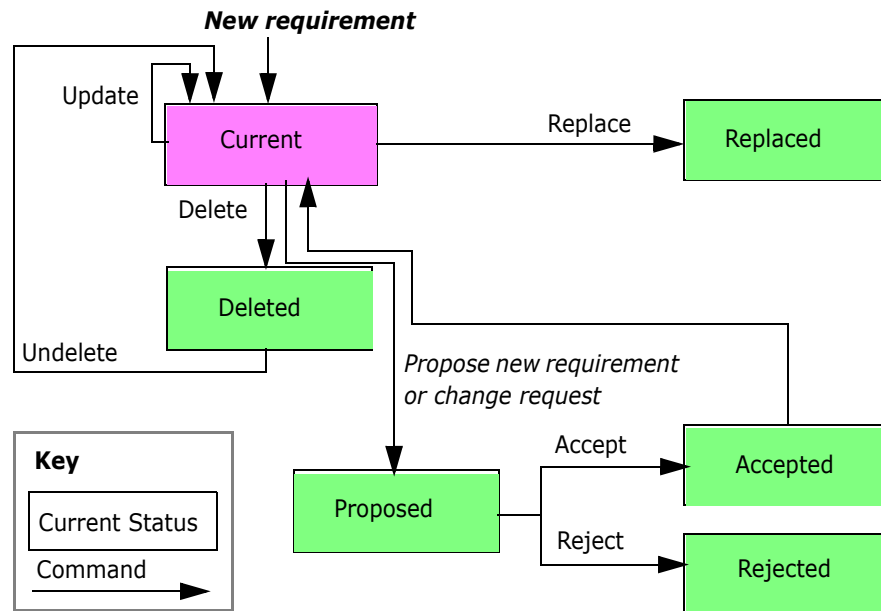
- **Delete**—The Delete command changes the Current Status of a requirement to Deleted, but leaves the requirement in the instance.
- **Undelete**—The Undelete command changes a Deleted requirement back to a Current requirement.
- **Remove**—The Remove command physically removes the requirement from the instance. Only requirements with the Current status can be removed. It is highly recommended that only instance administrators have permission to remove requirements.

When someone submits a change request to change a current requirement or create a new requirement, a copy of the current requirement is created with the current status of Proposed. There are two commands that can be used on a Proposed requirement:

- **Accept**—The Accept command accepts a proposed change. The current status of the proposed requirement becomes Accepted, and a copy of that requirement is created with the current status of Current.
- **Reject**—The Reject command rejects a proposed change. The current status of the proposed requirement becomes Rejected.

### Requirement Lifecycle

The requirement lifecycle is shown in the following illustration.



**Figure 1-5. Object Lifecycle**

## Requirement Views

You can view data in a source document from its native tool (for example, Microsoft Word). There are four other ways to view objects in Dimensions RM:

- Form view
- Grid view
- Paragraph layout
- Grid layout

### Form View

The form view displays one object at a time. From the form view you can edit object attributes. The form view is available from the Requirements View.

Dimensions RM generates a default form for each class based on its attribute definitions.

The following illustration shows the form view in RM Browser.

The screenshot shows the 'Form View' for a requirement object in the RM Browser. The title bar reads 'Marketing\_Requirements: MRKT\_000004'. Below the title bar is a navigation menu with tabs: ALL (selected), STANDARD, CUSTOM, SYSTEM, ATTACHMENTS, COMMENTS, LINKS, HISTORY, POLLS, and CONTAINERS. On the right side, there is a 'Category: RMDEMO' label. The main content area is divided into sections: 'STANDARD ATTRIBUTES' (expanded), 'CUSTOM ATTRIBUTES', 'SYSTEM ATTRIBUTES', 'ATTACHMENTS', 'COMMENTS', 'LINKS', 'HISTORY', 'POLLS', and 'CONTAINERS'. The 'STANDARD ATTRIBUTES' section contains the following information:

Rqmt ID:	Title:
MRKT_000004	Annotate photos with text
Text:	
The user shall be able to annotate their photos with textual descriptions. Annotation should include title, description and date of photograph.	

**Figure 1-6. Form View in RM Browser**

### Grid View

The grid view displays multiple objects in a table-like list. The column headings represent attributes of the object. The rows contain the data stored in the attributes. The following illustration shows the grid view in RM Browser.

Category	Containers	Rqmt ID	Title	Delivery Phase	Text
RMDEMO	ePhoto - Release 1.1, ePhoto Requiremen...	MRKT_000003	Runs on "standard" home PC	Build1	The ePhoto system shall be accessible to the user from a regular home PC environment ...
RMDEMO	ePhoto - Release 1.1, ePhoto Requiremen...	MRKT_000004	Annotate photos with text	Build3	The user shall be able to annotate their photos with textual descriptions. Annotation sho...
RMDEMO	Engineering Hot List, Ephoto Hot List, eP...	MRKT_000020	Provide photo special effects	TBD	The ePhoto system shall allow users to apply various special effects to photos.
RMDEMO	User	MRKT_000021	Border layouts provided	Build4	The ePhoto system shall allow users to display photos in various border layouts.

**Figure 1-7. Grid View in RM Browser**

### Paragraph Layout

The paragraph layout in the Document View of RM Browser displays requirements as paragraphs in a list.

**3.2 Miscellaneous Requirements**

Requirements Layout: [Editable Grid](#) | [Grid](#) | [Paragraph](#)

**3.2.1 System response times**

Suspect: No Rqmt ID: MRKT\_000029 Priority: High  
 Time Modified: 30-SEP-2015@01:54:24

The system response time shall not be greater than 3 seconds for 80 percent of the transactions.

**3.2.2 System weight**

Suspect: No Rqmt ID: MRKT\_000030 Priority: High  
 Time Modified: 30-SEP-2015@01:54:24

The system shall weigh less than 8 pounds.

**3.2.3 System comes in different colors**

Suspect: No Rqmt ID: MRKT\_000031 Priority: High  
 Time Modified: 30-SEP-2015@01:54:24

The system shall be available in a variety of colors.

**Figure 1-8. Paragraph Layout in Documents View in RM Browser**

### Grid Layout

The grid layout in the Document View of RM Browser displays multiple objects in a table-like list. The column headings represent attributes of the object. The rows contain the data stored in the attributes.

**3.2 Miscellaneous Requirements**

Requirements Layout: [Editable Grid](#) | [Grid](#) | [Paragraph](#)

#	Rqmt ID	Title	Text	Priority	Time Modified
3.2.1	MRKT_000029	System respon...	The system res...	High	30-SEP-2015...
3.2.2	MRKT_000030	System weight	The system sh...	High	30-SEP-2015...
3.2.3	MRKT_000031	System comes ...	The system sh...	High	30-SEP-2015...

**Figure 1-9. Grid Layout in Documents View of RM Browser**

## Queries

See chapter "Reports" in the *Dimensions RM Browser User's Guide*

## Query Terminology

As described earlier in this chapter, a relationship connects a primary and secondary class. Relationship constraints are logical expressions that are used to constrain searches. This section describes terminology and concepts that you encounter when you construct relationship constraints in queries.



**NOTE** Source and immediate relationships can be used to construct relationship constraints.

### Relationship Operators

The relationship operators PRIMARY\_IN and SECONDARY\_IN are used to identify objects that are either at the origin or termination of a link. The relationship operators NOT\_PRIMARY\_IN and NOT\_SECONDARY\_IN identify objects that may participate in such links, but do not. These operators are useful in locating objects that you are interested in linking. For example, given a relationship that connects system requirements to test cases, you could use the "not" operators to find requirements that are not associated with test cases.

### Source and Immediate Relationships

Source and immediate relationships are special relationships that are used to locate versions of objects.

- A *source* relationship refers to the original object in a chain of versions.
- An *immediate* relationship refers to the immediate predecessor or successor of an object.

### Relationship Operators in Source and Immediate Relationships

The following table lists relationship operators and describes their meanings in source and immediate relationships.

Operator	Source	Immediate
PRIMARY_IN	Requirements that have no parents (source requirements)	Requirements that have children (not the lowest level requirements)
SECONDARY_IN	Requirements that have no children (the lowest level requirements)	Requirements that have parents (derived requirements)
NOT_PRIMARY_IN	Requirements that have parents (derived requirements)	Requirements that have no children (the lowest level requirements)
NOT_SECONDARY_IN	Requirements that have children (not the lowest level requirements)	Requirements that have no parents (the source requirements)

## Reports

Reports are the results of queries made through scripts. You can create scripts to generate documents, traceability matrices, and other types of reports. Named scripts are stored in the database as instance resources and can be exported to the file system as text files where they can be used from the command line.

You can execute scripts from the command line or RM Browser. You can export the reports to files in a variety of formats, including Microsoft® Word, Microsoft® Excel®, Rich Text Format (RTF), Comma Separated Value (CSV), HTML, and XML.

## Containers

Containers are a higher grouping of any of the following objects:

- Baselines
- Collections
- Documents
- Snapshots

## Collections

Collections are a way to group objects of any class. Once a collection is created, it can be associated with an object by linking the object to the collection. Each object can be linked to many different collections, and each collection can be linked to many different objects. Collections can be referenced in scripts, making script creation simpler.

Parent collections contain child collections. Child collections contain objects. The hierarchy formed by the parent-child connections allows collections to be grouped into larger collections. For example, a parent collection called *Operations* can contain child collections for several types of operations, such as *Administrative*, *Storage*, and *Retrieval*.

A common use of collections is baselining. A baseline is a snapshot of objects at a particular time. You can create a collection called Baseline 1 that is a snapshot of all objects at the Alpha phase of the project. Later in the release cycle, you can create a collection called Baseline 2 that is a snapshot of all objects at the Beta phase. You can run reports that show the differences between objects in Baseline 1 and Baseline 2.

## Traceability and Impact Analysis

Links allow you to specify precisely which objects are related and why they are related. The relationships that you set up in your class definition diagram, and the corresponding links among objects that you subsequently create or import, form interconnections throughout your documents, models, test assets, and other work products. These physical connections model logical connections among the instance data.

Traceability and impact analysis are two ways you can analyze linkages. You can view traceability and impact analysis through reports run in RM Browser.

## Traceability

Different kinds of traceability result from different kinds of relationships. Relationships between different requirements classes can be used to show dependencies, such as the connection between operational requirements and software requirements.

Dimensions RM also manages relationships between successive versions of a particular object. This gives you the history of the object and allows you to trace its evolution through your project life cycle.

You can use traceability to answer questions about the completeness and consistency of your requirements management effort. Such questions include:

- How many operational requirements have not yet been addressed by software or hardware requirements?
- How many software requirements are not covered by test cases?
- How many requirements had successful tests for the current build?

## Impact Analysis

Having established traceability, you can perform impact analysis to examine the effects of certain changes. For example, if a particular system requirement is changed, what parts of the dependent software or hardware requirements are affected? What parts of the design, code, or test plan are affected? The answers to these questions help you scope the effort required to absorb requirements changes.

## Change Management

As discussed in "[Requirement Evolution](#)" on page 37, change management allows you to propose new objects or changes to existing objects, while keeping them separate from the existing objects. A proposed change object is an instance of the appropriate class, with its Current Status attribute set to Proposed.

Dimensions RM also provides a class type with which to build Engineering Change Proposals (ECPs). As you create a set of related proposed objects, you can link them to an ECP object so that they are easily accessible for review as a group.

## ALM Integration with Dimensions CM

The Application Lifecycle Management (ALM) integration lets you associate Dimensions RM requirements to Open Text Dimensions<sup>®</sup> CM requests. When you add a requirement to or remove a requirement from a collection, Dimensions CM is notified with the relevant information. Dimensions RM baselines flow to Dimensions CM, and Dimensions CM baselines flow to Dimensions RM.

You can associate:

- Multiple Dimensions RM instances to multiple Dimensions CM products.
- One or more Dimensions RM containers (baselines, collections, documents, or snapshots) to one or more Dimensions CM projects/streams.

For more information, see the common *Dimensions CM-Dimensions RM ALM Integration Guide*.

The above referenced guide also documents a Use Case for using Dimensions CM requests to augment Dimensions RM requirement management and traceability

## Sample Instances

Four sample instances are included with each Dimensions RM distribution. These samples must be installed by a Dimensions RM System Administrator, and provide a convenient way to get acquainted with the features of Dimensions RM.



**IMPORTANT!** Do NOT use the sample databases as a starting point for an actual production instance. Always create an instance of your own.

### The QLARIUS\_RM Sample Instance

The QLARIUS\_RM sample database lets business analysts and product managers quickly understand how the key functionality of Dimensions RM is beneficial in their own requirement lifecycles. QLARIUS\_RM demonstrates how requirements are categorized and stored, and how the requirements lifecycle is automated and enforced. QLARIUS\_RM provides predefined requirement classes, links between classes, and built-in reporting.

The default users and passwords for the QLARIUS\_RM instance are listed in the following table.

QLARIUS_RM		
User Name	Password	Administrator
DEV	rtm	Yes
DMSYS	rtm	Yes
EPHOTO	rtm	Yes
MARK	mark	No
PETA	peta	No
QLARIUS_RMADMIN	rtm ( <i>SQL Server only</i> )	Yes (Instance)
QUIN	quin	No
SALLY	sally	No
TED	ted	No

### The RMDEMO Sample Database

RMDEMO is another sample database that provides a rich set of Dimensions RM features and functionality.

The default users and passwords for the RMDEMO instance are listed in the following table.

RMDEMO		
User Name	Password	Administrator
ADMINISTRATION	rtm	No
BUSINESS_ANALYST	rtm	No
DEV	rtm	Yes
DEV_MANAGER	rtm	No
DEVELOPMENT	rtm	No
ENGINEERING	rtm	No
EPHOTO	rtm	Yes
EPHOTO_INFO	rtm	No
JOE	rtm	Yes
MANAGEMENT	rtm	No
MARKETING	rtm	No
PRODUCT_MANAGER	rtm	No
PROJECT_MANAGER	rtm	No
QA	rtm	Yes
RMDEMOADMIN	rtm (SQL Server only)	Yes (Instance)
RTMADMIN	rtm	Yes
SALES	rtm	No
SUPPORT	rtm	No
TECH_PUBS	rtm	No
TEST	rtm	No
TEST_MANAGER	rtm	No
TRAINING	rtm	No

## The AGILE\_RMDEMO Sample Database

AGILE\_RMDEMO is sample database that provides a rich set of Agile Dimensions RM features and functionality.

The default users and passwords for the AGILE\_RMDEMO instance are listed in the following table.

AGILE_RMDEMO		
User Name	Password	Administrator
ADMINISTRATION	rtm	No
AGILE_RMDEMOADMIN	rtm (SQL Server only)	Yes (Instance)
BUSINESS_ANALYST	rtm	No

AGILE_RMDEMO		
User Name	Password	Administrator
DEV	rtm	Yes
DEV_MANAGER	rtm	
DEVELOPMENT	rtm	No
ENGINEERING	rtm	No
EPHOTO	rtm	Yes
EPHOTO_DEV	rtm	No
EPHOTO_INFO	rtm	Yes
EPHOTO_LEAD	rtm	No
EPHOTO_PO	rtm	No
JOE	rtm	Yes
MANAGEMENT	rtm	No
MARKETING	rtm	No
PRODUCT_MANAGER	rtm	No
PROJECT_MANAGER	rtm	No
QA	rtm	Yes
RTMADMIN	rtm	Yes
SALES	rtm	No
SUPPORT	rtm	No
TECH_PUBS	rtm	No
TEST	rtm	No
TEST_MANAGER	rtm	No
TRAINING	rtm	No

## The ALM\_DEMO Sample Database

ALM\_DEMO is sample database that provides a rich set of Dimensions RM features and functionality in the context of application lifecycle management.

The default users and passwords for the ALM\_DEMO instance are listed in the following table.

AGILE_RMDEMO		
User Name	Password	Administrator
ALM_DEMOADMIN	rtm (SQL Server only)	Yes (Instance)
ASCHOEJ4	rtm	No
DEV	rtm	Yes
DMSYS	rtm	Yes
EPHOTO	rtm	Yes

AGILE_RMDEMO		
User Name	Password	Administrator
JENS	rtm	No
JOANNA	rtm	No
JOE	rtm	Yes
JUTTA	rtm	No
KAY	rtm	No
LARS	rtm	No
MARTIN	rtm	No
PM	rtm	No
RTMADMIN	rtm	Yes

## Database Accounts Used by Dimensions RM

Each Dimensions RM database requires two accounts in order to operate:

- ICDBA
- ICADMIN

Additional user accounts are created for each Dimensions RM instance, such as RMDEMO, QLARIUS, etc. Each new Dimensions RM instance creates a new user account. The instance accounts are schema owners in database.

### ICDBA Account

Dimensions RM requires system level access to create **ICDBA**. After that, all database level DBA functions are performed by ICDBA. When the first instance is created, the ICADMIN account is created - these accounts work together at the database and instance levels.

Dimensions RM is designed not to require an Database Administrator (DBA); the RM administrator can, in most cases, perform the necessary maintenance functions without requiring hands on database access. However, organizations with DBAs managing all databases, can support the RM admin when the database is created, provide access to create the ICDBA account - and then leave them to it.

For information on creating the ICDBA account, see ["Creating the ICDBA Account" on page 161](#).

### Accounts Granted the Oracle RESOURCE Role

When RM Manage performs Oracle maintenance (such as recreating database indexes, database procedures, and instance triggers), the ICADMIN, and ICDBA user accounts and the RTM\_USER profile are granted the RESOURCE role.

## Locking RM Oracle User Accounts

Dimensions RM Oracle accounts generally cannot be locked without causing problems. The following list indicates the problems associated with locking the various accounts:

- **ICADMIN:** If locked, Dimensions RM will not function.
- **ICDBA:** It has been reported that some customers have locked the ICDBA account until it is needed for RM Manage functions. While the account is locked, RM Manage and Class Definition will sometimes throw exceptions and errors--putting all RM administrative functions at risk of failure. The user interface appeared to function without issue. This is **NOT** a supported or tested configuration.

The recommended approach to protect DBA access is to change the ICDBA password to something unknown to the Dimensions RM team. During the brief times when RM needs access to perform maintenance, change the password back to the one expected by RM. After the maintenance is complete, change the password back to something unknown to the RM administration team.

- **RM Instances:** There is one account of this type for every RM instance. You can lock users out of the database and prevent access to all instance data by locking the instance accounts. If a user tries to access Dimensions RM instance data while the instance account is locked, they will receive errors.

## Chapter 2

---

# Customizing Web Forms and Templates

Customizing Web Forms	50
Defining Custom Styles for Exported Documents	61
Creating Templates to Export Requirements	63
Defining Headers and Footers for Exported Documents	65
Exporting a Document with File Attachments from a Separate Server	67
Customizing RM Browser Menus and Title Bars	68
Changing the Default Settings of the RM Browser Text Editor	73
Customizing the Editable Grid	73
Configuring the Expansion and Collapse of RM Browser Sections	74
Creating Custom Login Alert Pages for RM Browser	74
Customizing Headers and Footers of RM Browser Interface	75
Dashboard Export	76

# Customizing Web Forms

## Important Change to Web Forms Management

The forms used to display the data stored with each RM class is now being managed inside the RM Database. The definition and modification of the forms themselves can be accomplished from the Dimensions RM Browser, please see the *Dimensions RM Browser User's Guide* for instructions.

The instructions will remain in Administrator's Guide for those teams who wish to continue maintaining Class forms. They can still be downloaded, modified and managed by the administrator.

## Template Processing

A templates directory (<RM Install Dir>\Dimensions 25.2\Common Tools 2.4.0.0\tomcat\9.0\webapps\rtmBrowser\forms) contains the template files for all custom forms.

Each database and instance can have its own set of template files. A template file represents the custom layout for a single class type within the instance. The forms are stored in folders name for the database and the instance. For example, if the database name is **CDRM** and then Instance is **ALM\_DEMO** the forms will be stored in: ...\\forms\CDRM\ALM\_DEMO.

The templates are processed as follows:

- 1 RM Browser looks for a class-specific XML file, and loads the file if found.
- 2 If a class-specific XML file is not found, RM Browser looks for the default file for the instance (forms\database\instance\default.xml), and loads it if it is found.
- 3 If an instance-specific XML file is not found, RM Browser loads the global default file (<RM Install Dir>\Dimensions 25.2\Common Tools 2.4.0.0\tomcat\9.0\webapps\rtmBrowser\forms\common\default.xml). This file creates a standard Dimensions RM appearance.

The default forms used by Test Management (Test\_Run\_Step.xml, Test\_Step.xml) are also stored in the global default forms\common.

The naming of the database and instance directories must match their visible names. Template file names match the class name with a ".xml" extension.



**NOTE** If you rename a database, instance, or class, you must rename the template directories or files.

## Template Layout

As mentioned earlier, the template layout is an XML file.

The following illustration shows the layout of the global default file (the file that ships with Dimensions RM). This form applies to classes across instances.

```
<?xml version="1.0" encoding="UTF-8"?>
<form xmlns="http://schemas.serena.com/2005/01/rtmform" animationspeed="1">
  <section type="prioritized"/>
  <section type="standard"/>
  <section type="custom"/>
  <section type="groupattribute"/>
  <section type="system"/>
  <section type="attachments"/>
  <section type="comments"/>
  <section type="links"/>
  <section type="history"/>
  <section type="polls"/>
  <section type="dimensions"/>
  <section type="container"/>
  <section type="workflowhistory"/>
  <section type="provide"/>
</form>
```

The following illustration shows the layout of an example user-defined XML file that is specific to a single class name within an instance. The table that follows the illustration describes the tags in the file. The table is ordered logically, rather than by the appearance of the tags in the XML file.

```

1      <?xml version="1.0" encoding="UTF-8"?>
2      <form xmlns="http://schemas.serena.com/2005/01/rtmform" animationspeed="5">
3          <script src="../jscript/myCustomScript.js"/>
4          <stylesheet src="../cssmyCustomStylesheet.css"/>
5          <section type="user" label="My First Section" cols="3" labelplacement="top">
6              <attribute id="ACTUAL_FIX_TIME"/>
7              <attribute id="DESCRIPTION" colspan="2"/>
8              <group label="Release Information" cols="2" labelplacement="left"
9                  expandable="no">
10                 <attribute id="RELEASE_ID" label="Id"/>
11                 <attribute id="RELEASE_DATE" label="Date"/>
12                 <attribute id="RELEASE_STATUS" label="Status"/>
13             </group>
14             <text><![CDATA[<a href="http://www.serena.com"></a>]]></text>
16         </section>
17         <section type="user" label="My second Section" cols="2">
18             <attribute id="RESPONSIBLE_ANALYST" type="Custom" label="Analyst"
19                 colspan="2">
20                 <writeable>
21                     <xhtml>
22                         <input name="myField" type="text" value="" size="30" maxlength="10"
23                             onchange="dosomethingspecial()" onfocus="dosomethingspecial()" />
24                         <button type="button" id="myButton"
25                             onclick="dosomethingspecial()">Search...</button>
26                     </xhtml>
27                 </writeable>
28             </attribute>
29         </section>
30         <section type="prioritized"/>
31         <!--
32         <section type="standard" label="Standard Attributes"/>
33         <section type="custom" label="Custom Attributes"/> -->
34         <section type="groupattribute" label="Group Attributes"/>
35         <section type="system" label="My System"/>
36         <section type="attachments" label="File Attachments"/>
37         <section type="comments" label="Discussions"/>
38         <section type="links" label="Relationships"/>
39         <section type="history" label="History"/>
40         <section type="polls" label="Polls"/>
41         <section type="dimensions" label="Dim CM Associations" />
42         <section type="container"/>
43     </form>

```



**CAUTION!** Attributes can only be defined in one section.

Tag	Description
1	<p>Sections in forms are set by default to open and close by a scrolling mechanism. The <code>animationspeed</code> option determines one of the following:</p> <ul style="list-style-type: none"> <li>■ The speed of the scrolling (default <code>animationspeed=0</code>)</li> <li>■ Whether the scrolling mechanism is used. If it is not used (<code>animationspeed=0</code>), the sections open and close immediately when the user clicks <b>+</b> or <b>-</b>.</li> </ul> <p>For information about how to configure the <code>animationspeed</code> option, see <a href="#">"Configuring the Expansion and Collapse of RM Browser Sections" on page 74</a>.</p>
2	<p>The <code>&lt;script&gt;</code> tag contains a user-defined JavaScript file. You can include more than one JavaScript file.</p> <p>If a custom JavaScript file needs to perform processing after the form loads, unloads, gains focus, or loses focus, you can hook into the standard JavaScript <code>onload</code>, <code>onunload</code>, <code>onfocus</code>, and <code>onblur</code> events. These are dialog specific and occur after the form finishes its own processing of these events.</p> <p>The function names for each form follow:</p> <p><b>New Requirement, Edit Attributes, Change Request, Comments, Form View, Documents View:</b> <code>objOnLoad</code>, <code>objOnUnload</code>, <code>objOnFocus</code>, <code>objOnBlur</code>, <code>objHistoryOnLoad</code> (<b>NOTE:</b> The Documents View form is displayed only after you click a requirement in the navigation tree.)</p> <p><b>Query by Class, Query by Relationship:</b> <code>queryOnLoad</code>, <code>queryOnUnload</code>, <code>queryOnFocus</code>, <code>queryOnBlur</code></p> <p><b>Edit Query:</b> <code>editQueryOnLoad</code> (<b>NOTE:</b> This function is called after editing an existing query in the Query by Class or Query by Relationship dialogs after the field data has been entered.)</p> <p><b>Link Objects:</b> <code>linkOnLoad</code>, <code>linkOnUnload</code>, <code>linkOnFocus</code>, <code>linkOnBlur</code></p> <p><b>Organize by Collection:</b> <code>collOnLoad</code>, <code>collOnUnload</code>, <code>collOnFocus</code>, <code>collOnBlur</code></p> <p><b>Approve Change Request:</b> <code>crOnLoad</code>, <code>crOnUnload</code>, <code>crOnFocus</code>, <code>crOnBlur</code></p> <p><b>Organize by Category:</b> <code>catOnLoad</code>, <code>catOnUnload</code>, <code>catOnFocus</code>, <code>catOnBlur</code></p> <p><b>Add to Chapter:</b> <code>atcOnLoad</code>, <code>atcOnUnload</code>, <code>atcOnFocus</code>, <code>atcOnBlur</code></p> <p>There are other JavaScript functions that you can use with query-style forms and other forms that contain attributes. See <a href="#">"Query-Style Form Functions" on page 55</a> and <a href="#">"Helper Functions" on page 58</a> for details.</p> <p>The <code>rtmObjCustomHtmlPrint(attrName)</code> function is called for any custom HTML attribute to get the read-only (print) value. The <code>attrName</code> parameter is the internal attribute name.</p> <p>The return value is a string that contains that value, which can be any HTML text or plain text that is used in the printed page to represent the value of that attribute.</p> <p>This function applies to the <b>New Requirement</b> and <b>Edit Attributes</b> dialog boxes only.</p>
3	<p>The <code>&lt;stylesheet&gt;</code> tag contains a user-defined stylesheet. You can include more than one stylesheet tag.</p>


Tag	Description
<b>4</b>	<p>The <code>&lt;section&gt;</code> tag contains either a predefined section or a user-defined section.</p> <p>A predefined section contains a type, a label (defaults to the standard title for the section), the label placement (left or top; defaults to left), and the number of columns (defaults to two). A predefined section contains no other elements.</p> <p>Predefined section types include standard, custom, system, attachments, comments, links, history, polls, and dimensions.</p> <p>Predefined section types are used in the template (.xml) file. You can rearrange the placement of these sections.</p> <p>If a predefined type exists within the template file but would not normally be shown for an object, it is not displayed. If a predefined section does not exist within the template file, the section is not displayed.</p> <p>A user-defined section allows you to specify the order and grouping of attributes, and allows you to place custom fields on the form. A user-defined section contains a specific type (that is, "user"), a label, the label placement (left or top; defaults to left), and the number of columns (defaults to two). The label is the section label, but the label placement refers to attribute labels within that section.</p>
<b>5</b>	<p>The <code>&lt;attribute&gt;</code> tag can specify a standard attribute or a custom field that populates an attribute. The layout of the fields within a section or group is from left to right. You can specify a custom label or use the default label for the attribute from the database. You can also specify the placement of the label (left or top, defaults to whatever the group or section is set to). The label is the section label, but the label placement refers to attribute labels within that section.</p> <p>You can specify a custom attribute type. RM Browser automatically generates a hidden attribute associated with a custom field by using the <code>attribute id</code> that is provided. You can specify how many columns the field consumes (defaults to one).</p> <p>See the description for tag 9 for options when you use XHTML/HTML inside an <code>&lt;attribute&gt;</code> tag.</p>
<b>6</b>	<p>The <code>&lt;group&gt;</code> tag allows you to physically group attributes, but in the confines of a section. A section could have several different groupings of attributes.</p> <p>The group specifies the attributes contained in it, a label, the label placement (left or top; defaults to left), the number of columns (defaults to two), and whether it is expandable or not (defaults to not expandable).</p>
<b>7</b>	<p>The CDATA element can be used in <code>&lt;text&gt;</code> and <code>&lt;attribute&gt;</code> tags. It is used to insert HTML that is not well formed into an XML file. Use CDATA if you do not know that the additional text is XHTML compliant.</p>

Tag	Description
8	<p>The <code>&lt;writeable&gt;</code> tag contained in the attribute definition indicates that if the form is displayed for editing, this is the XHTML/HTML that will be used. Alternatively, a <code>&lt;read-only&gt;</code> tag means that if the form is displayed as read-only, this is the XHTML/HTML that will be used. It is your responsibility to transfer data to a hidden field.</p> <p>You have three options when you use XHTML/HTML:</p> <ul style="list-style-type: none"> <li>■ The custom XHTML/HTML can apply to both editable and read-only forms (if specified directly inside the <code>&lt;text&gt;</code> or <code>&lt;attribute&gt;</code> tag).</li> <li>■ Different XHTML/HTML can be provided for editable as opposed to read-only forms (if specified in <code>&lt;writeable&gt;</code> and <code>&lt;read-only&gt;</code> elements inside the <code>&lt;text&gt;</code> or <code>&lt;attribute&gt;</code> tag).</li> <li>■ The XHTML/HTML can only apply to editable forms (if specified in <code>&lt;writeable&gt;</code> only elements inside the <code>&lt;text&gt;</code> or <code>&lt;attribute&gt;</code> tag). With this option, read-only forms display the attribute in the standard way.</li> </ul> <p>The <code>&lt;writeable2&gt;</code> tag and <code>&lt;readonly2&gt;</code> tag are the same as the <code>&lt;writeable&gt;</code> tag and <code>&lt;readonly&gt;</code> tag, except that they are used whenever a range control is shown (any query-style dialog when <b>between</b> or <b>not between</b> is the selected operator). If these tags are not present, then the <code>&lt;writeable&gt;</code> tag and <code>&lt;readonly&gt;</code> tag are used for both controls. However, this is generally not recommended because it provides no way to specify a unique control ID and could cause the custom JavaScript to work in unexpected ways.</p>
9	<p>The <code>&lt;xhtml&gt;</code> tag can be used in <code>&lt;text&gt;</code> and <code>&lt;attribute&gt;</code> tags. It allows you to insert XHTML-compliant code that adds elements such as buttons to the form.</p> <p>You can also add text boxes inside <code>&lt;xhtml&gt;</code> tags with sizes set to any number of columns and rows, optionally with scrolling. For example, the following tag:</p> <pre data-bbox="555 1171 1345 1329">&lt;xhtml&gt; &lt;TEXTAREA name="New_custom11" id="new_id11" rows="4" cols="25" wrap="off"&gt; &lt;/TEXTAREA&gt; &lt;/xhtml&gt;</pre> <p>Adds a text box that allows four rows and 25 columns (in characters). The <code>wrap="off"</code> attribute enables scrollbars for this text box.</p>

### Query-Style Form Functions

The following functions can be used to customize the **Attribute Constraints** tab on query-style dialogs. They can be used to either change the form or the lists that appear when you hover over the down arrow button ▾ on either side of an attribute control. Query-style dialog boxes include:

- **Query by Class**
- **Query by Relationship**
- **Organize by Category**
- **Link**
- **Organize by Collection**
- **Add to Chapter**

The following functions can be used to customize query-style form lists that appear when you hover over the down arrow button  on either side of an attribute control.

Function	Description
<code>rtmQueryOnOperatorSelection(attrId, operator)</code>	Called whenever an operator is selected in any query-style dialog. This function must return <code>true</code> if the selection is allowed or <code>false</code> if it is not allowed.
<code>rtmQueryOnValueOptionSelection(attrId, option)</code>	Called whenever a value option is selected in the list that opens to the right of the attribute control ( <b>Query by Class</b> and <b>Query by Relationship</b> only). This function must return <code>true</code> if the selection is allowed or <code>false</code> if it is not allowed.
<code>rtmQueryAddCustomAttributeOperators(attrId)</code>	Called for any Web form custom attribute because the default operator list may or may not be appropriate. It should define the list in the same way as the <code>rtmQueryAdd...</code> functions, or may simply call one of them to get the same list. The <code>rtmQueryAdd...</code> functions are listed below: <ul style="list-style-type: none"> <li>■ <code>rtmQueryAddAlphaOperators</code></li> <li>■ <code>rtmQueryAddNumericOperators</code></li> <li>■ <code>rtmQueryAddDateOperators</code></li> <li>■ <code>rtmQueryAddListOperators</code></li> <li>■ <code>rtmQueryAddTextOperators</code></li> </ul> and are defined in <code>icObjectFormsMenus.js</code> (located in <code>&lt;RM Install Dir&gt;\rtmBrowser\rm\common\js</code> ). To customize the operator list, use the <code>rtmQueryAdd...</code> functions to build the list the way you want. Use the calls at the end of the functions to set the default operator. These calls include <code>rtmQueryLike</code> and <code>rtmQueryIn</code> .
<code>rtmQueryAddCustomAttributeOperators(attrName)</code>	Called for custom attributes when a query constraints dialog box that contains that attribute is opened.
<code>rtmQueryGetCustomValues(attrId, operator)</code>	Called whenever a query-style dialog is generating a script for each attribute. This function should generally not be necessary, but is provided in case the default processing is not sufficient. This function must return an array of values for any attributes using custom processing and <code>null</code> for any attributes using the default processing.

Function	Description
<code>rtmQuerySetCustomValues(attrId, values)</code>	Called to set <b>in</b> and <b>not in</b> custom attributes when loading an existing query for editing. This function is used in the case where a custom Web form hides an attribute that is part of an IN clause. When this occurs, Dimensions RM checks for the existence of the function and calls it so that the custom JavaScript can set the custom control to the correct value or values. This function returns true if the attribute was handled and false if it was not handled.
<code>rtmQueryShowValueOptions(attrId)</code>	Called to tell Dimensions RM to not show the list that opens to the right of the attribute control and contains the <b>Fixed</b> or <b>Entered at runtime</b> options.

### Query-Style Form Function Parameters

The parameters for the ["Query-Style Form Functions" on page 55](#) are described in the following table.

Parameter	Description
<code>attrId</code>	The attribute name with the dialog name appended to it. This parameter is used to uniquely identify an attribute. For example, PUIDQryRS or PUIDQryRT for the PUID on the <b>Constraints-Source</b> or <b>Constraints-Target</b> tabs on the <b>Query by Relationship</b> form.
<code>operator</code>	A string with the internal operator (LIKE, IN, INITIALIZED, and so on) or pseudo-operator (BETWEEN and NOT BETWEEN).
<code>option</code>	FIXED (specified during the creation of the script) or RUNTIME (specified by the user in response to a prompt during the execution of the script).
<code>values</code>	The values in the IN list of the script.

## Helper Functions

The following functions are helper functions for Web form custom attributes. They are used to get and set the attribute values that Dimensions RM uses.

Function	Description
<code>rtmUtilGetAttributeElementId</code> ( <code>attrId</code> , <code>isRangeCtrl</code> )	Builds an ID string based on the attribute name and the context from which it is being called. This function is not validated.
<code>rtmUtilGetAttributeValue</code> ( <code>attrId</code> , <code>isRangeCtrl</code> )	Gets the value of the specified attribute from the Web form. If the element (as determined by <code>rtmUtilGetAttributeElementId</code> ) is an INPUT tag (whether it was defined in a custom or standard section), it returns its value. Otherwise, it returns the innerHTML value of the element. If the attribute is not found, the function returns null.
<code>rtmUtilSetAttributeValue</code> ( <code>attrId</code> , <code>value</code> , <code>isRangeCtrl</code> )	Sets the value of the specified attribute.

## Helper Function Parameters

The parameters for the ["Helper Functions" on page 58](#) are described in the following table.

Parameter	Description
<code>attrId</code>	The attribute name. This parameter is used to uniquely identify an attribute.
<code>value</code>	A string value to put into the Dimensions RM attribute in the Web form. This parameter does not work for non-Dimensions RM attributes.
<code>isRangeCtrl</code>	Valid values are <code>true</code> or <code>false</code> . This parameter is used with ranges (BETWEEN and NOT BETWEEN) that have two controls for a single attribute. The parameter would be <code>true</code> to show the second control.

## Customizable Web Forms

The behavior of customized Web forms falls into two categories.

## Editable Mode

Web Page	Behavior
New Requirement Edit Requirement Change Request Query by Class Query by Relationship Link Requirements Organize by Collection Organize by Category Add to Chapter	Each of these forms use the user-defined template for the object in "editable" mode with respect to customized attribute fields. For custom user fields, the "editable" XHTML/HTML that you provided is displayed. The header and footer sections of these forms are not customizable.

## Read-Only Mode

Web Page	Behavior
Comments Form View Approve Change Request Documents View Traceability View	Each of these forms use the user-defined template for the object in "read-only" mode with respect to customized attribute fields. They display the layout without any user-editable fields. For custom user fields, they display either the "read-only" XHTML/HTML that you provided, or if none, the value of the specified field. If there is no <writeable> or <read-only> tag, the same XHTML/HTML is displayed in both editable and read-only forms. The header and footer sections of these forms are not customizable. <b>NOTE:</b> The Documents View and Traceability View forms are displayed only after you click a requirement in the navigation tree or traceability tree.

## Allowable Tags

The following listing shows the allowable tags that you can use when customizing Web forms.

<script>:

src - URL to JavaScript file

<stylesheet>:

src - URL to Cascading Style Sheet (CSS) file

<section>:

labelplacement - left or top (whether label is placed beside or above attribute value)

cols - number of attribute columns within the section

header - yes or no (whether to show the expandable section header or not)

justified - left or right (how to justify an attribute within the attribute column)

section type - prioritized, standard, custom, groupattribute, system, attachments, comments, links, history, polls, dimensions, container, workflowhistory, provide

user section tags:

<attribute>:

id - attribute name (not display name)

colspan - number of attribute columns occupied by this attribute

type - field or custom (field shows the attribute in the standard way)

custom attribute tags:

<readonly> - how the custom attribute gets displayed in read-only forms (for example, plain text)

<xhtml> - for well-formed HTML

<![CDATA[]]> - for standard HTML (not well-formed HTML)

<writeable> - how the custom attribute gets displayed in editable requirement forms

<xhtml> - for well-formed HTML

<![CDATA[]]> - for standard HTML (not well-formed HTML)

**NOTE:** If neither custom attribute tag is used, the contents apply to both editable and read-only forms.

<group> (a subgroup within a section):

cols - number of attribute columns within a section

expandable - yes or no (whether the group can be expanded and collapsed or displayed in a fieldset)

tags: <attribute> and <text>, just like in <section>

<text>:

colspan - number of attribute columns occupied by this attribute

type - if set to "url", generates and displays the URL to the requirement. For example, <text label="Requirement Link" type="url"/>

tags: <xhtml> and <![CDATA[]]>, just like in <attribute>

# Defining Custom Styles for Exported Documents

The basic reason you define custom styles is to change the style of chapter and requirement headings. However, you can customize any styles that are used in a document unless they are used as in-line styles. (Some of the styles introduced when you edit a requirement using the HTML editor in RM Browser are in-line styles and cannot be changed.)



**IMPORTANT!** Using custom styles is only supported if the chapter is formatted as **Paragraph**. To ensure that all chapters formatted as **Paragraph** follow these steps:

- 1 Open the document in Document View.
- 2 Click on **Format Document** in the **Documents** group in the **Action** pane.
- 3 **Requirement Layout:** Select **Paragraph**.
- 4 Click the **Reset all chapters** button.
- 5 Click the **OK** button.

## To define custom styles:

- 1 Create or open a Microsoft Word document that contains the template format.
- 2 Save the Word document as filtered HTML document.



**IMPORTANT!** You must set the file **Save as type** in Word to: **Web Page, Filtered (\*.htm;\*.html)**.

Do **NOT** select "Single File Web Page (\*.mht;\*.mhtml)" or "Web Page (\*.htm;\*.html)".



**NOTE** This is the only chapter which requires to save the file using Web Page, Filtered. The chapters [Creating Templates to Export Requirements](#) and [Defining Headers and Footers for Exported Documents](#) require a different format.

- 3 If it does not exist, create the directory *DataBase\_Name* in this directory  
`<RM Install Dir>\Dimensions 25.2\Common Tools  
2.4.0.0\tomcat\9.0\webapps\rtmBrowser\conf`



**NOTE** *Database\_Name* is identical with the database name from the login dialog.

- 4 If it does not exist, create the directory *Instance\_Name* inside the *DataBase\_Name* directory from [Step 3](#).



**NOTE** *Instance\_Name* is identical with the instance name from the login dialog.

- 5 In a text editor, create a file named `DocumentPublishTemplate.txt`.

- 6 Decide if you want to use the `DocumentPublishTemplate.txt` file for all export processes or with a specific publish template:
- a All export processes:** Place the `DocumentPublishTemplate.txt` file into the following directory:
- ```
<RM Install Dir>\Dimensions 25.2\Common Tools
  2.4.0.0\tomcat\9.0\webapps\rtmBrowser\conf\
    Database_Name\Instance_Name
```
- b With a specific publish template:** Create the marked directories in path `<RM Install Dir>\Dimensions 25.2\Common Tools 2.4.0.0\tomcat\9.0\webapps\rtmBrowser\conf\ Database_Name\Instance_Name\publish templates\TemplateName` and place `DocumentPublishTemplate.txt` into the `TemplateName` directory.



**NOTE** Using `DocumentPublishTemplate.txt` with a specific publish template overrides the `DocumentPublishTemplate.txt` file for all export processes.

- 7 Open the HTML file you created in step 2 in text editor (e.g. Notepad).
- 8 The HTML file might contain more than one style section. Some of these style sections might be surrounded by an HTML comment (`<!--` and `-->`). You need to copy all styles and include their `<style>` and `</style>` tags as well as the HTML comments if applicable and paste them into the `DocumentPublishTemplate.txt` file.



**NOTE**

- Include the `<style>` and `</style>` tags in the text that you copy. A style section might look like this:
 

```
<style>
<!--
/* Font Definitions */
@font-face
{font-family:"Cambria Math";
panose-1:2 4 5 3 5 4 6 3 2 4;
mso-font-charset:1;
mso-generic-font-family:roman;
mso-font-format:other;
mso-font-pitch:variable;
mso-font-signature:0 0 0 0 0 0;}
...
</style>
```
- If a style is surrounded by an HTML comment (`<!--` and `-->`), the comment tags must be copied as well. A commented style definition might look like this:
 

```
<!--[if gte mso 10]>
<style>
/* Style Definitions */
...
</style><![endif]>
```

- 9 Find the text `WordSection1` and replace it with **Section1**. You should be offered these texts:
- ```
@page WordSection1
div.WordSection1
{page:WordSection1;}
```

- 10 Save the file DocumentPublishTemplate.txt.

## Creating Templates to Export Requirements

There can be many templates for each instance. Each template is contained in the Publish Templates directory. This directory contains files that provide formatting for requirements from any class that you want to customize. This directory can also contain style, header and footer files.



**IMPORTANT!** Using templates is only supported if the chapter is formatted as **Paragraph**. To ensure that all chapters formatted as **Paragraph** follow these steps:

- 1 Open the document in Document View.
- 2 Click on **Format Document** in the **Documents** group in the **Action** pane.
- 3 **Requirement Layout:** Select **Paragraph**.
- 4 Click the **Reset all chapters** button.
- 5 Click the **OK** button.



**NOTE** These templates are not related to form templates (chapter "[Customizing Web Forms](#)" on page 50).

Users can select the template to be used for each document using the **Format Document** dialog box in Documents View.



**NOTE** You must select **Paragraph** in the **Requirement Format** section of the **Format Document** dialog box, not **Grid**.

### To create a new requirement template:

- 1 Create or open a Microsoft Word document that contains the template format.
- 2 Add attribute names (not attribute display names) as placeholders for the content of an attribute.

The following illustration shows an example of a portion of such a Word document.

|                  |            |                        |                  |
|------------------|------------|------------------------|------------------|
| <b>Priority:</b> | <PRIORITY> | <b>Delivery Phase:</b> | <DELIVERY_PHASE> |
| <TITLE>          |            |                        |                  |
| <TEXT>           |            |                        |                  |



**IMPORTANT!** When applying formatting to attribute names, <ATTRIBUTE>, you **MUST** select the entire attribute name **including** the angle brackets, < >. Otherwise the attribute name and angle brackets will be exported rather than the value of the attribute.



**NOTE** If you use a paragraph instead of a table, you might want to use numbering like with chapters. In this case, use the **<#HEADING\_NUMBER#>** placeholder before the title, e.g. **<#HEADING\_NUMBER#> <TITLE>**.

**3** Save the Word document in HTML format.



**IMPORTANT!**

- The file name must match the name of the class.
- You must set the file **Save as type** in Word to: **Web Page (\*.htm;\*.html)**. Do **NOT** select "Single File Web Page (\*.mht;\*.mhtml)" or "Web Page, Filtered (\*.htm;\*.html)".

**4** Use Windows Explorer to manually change the file extension to:  
.txt

**5** Open the text file with a text editor (e.g. Notepad)

**6** Find the text *WordSection1* and replace it with **Section1**. You should be offered these texts:

```
@page WordSection1
div.WordSection1
{page:WordSection1;}
```

**7** Find all directory references of *WordFileName\_files* and rename *WordFileName\_files* to **PublishDoc\_files**.

**8** If it does not exist, create the directory *DataBase\_Name* in this directory  
*RM\_Install\Common Tools #.#\tomcat\#.#\webapps\rtmBrowser\conf*



**NOTE** *DataBase\_Name* is identical with the database name from the login dialog.

**9** If it does not exist, create the directory *Instance\_Name* inside the *DataBase\_Name* directory from [Step 8](#).



**NOTE** *Instance\_Name* is identical with the instance name from the login dialog.

**10** If it does not exist, create the directory *publish templates* inside the *Instance\_Name* directory from [Step 9](#).

**11** Copy the .txt file and the *WordFileName\_files* directory to the following location:

```
RM_Install\Common Tools #.#\tomcat\#.#\webapps\rtmBrowser\conf
  \DataBase_Name\Instance_Name\publish templates\TemplateDirectory
  \ClassName.txt
```

Where *TemplateDirectory* is the name you want displayed in the **Publish Requirement Template** list on the Format Document dialog.

- 12** The template is now available for users to select. Repeat this procedure for each class for which you want a custom template.



**NOTE** If there are files in the following directory:

```
RM_Install\Common Tools #.#\tomcat\#.#\webapps\rtmBrowser\conf
  \DataBase_Name\Instance_Name\publish templates\TemplateDirectory
```

They are used and are available from the **Format Document** dialog box from the **Documents View Actions pane**. If this directory is empty, the style and header files defined for each instance (if any) in the following directory are used:

```
RM_Install\Common Tools #.#\tomcat\#.#\webapps\rtmBrowser\conf
  \DataBase_Name\Instance_Name
```

For information about creating the style and header files in the latter case, see ["Defining Custom Styles for Exported Documents" on page 61](#) and ["Defining Headers and Footers for Exported Documents" on page 65](#).

## Defining Headers and Footers for Exported Documents

By default, no header and footer information is exported from Document View in RM Browser. This is the case even if the document you imported from RM Import has a header and footer.

You can define header and footer information to be included in such documents.



**IMPORTANT!** Using headers and footers is only supported if the chapter is formatted as **Paragraph**. To ensure that all chapters formatted as **Paragraph** follow these steps:

- 1 Open the document in Document View.
- 2 Click on **Format Document** in the **Documents** group in the **Action** pane.
- 3 **Requirement Layout:** Select **Paragraph**.
- 4 Click the **Reset all chapters** button.
- 5 Click the **OK** button.



**NOTE** The methods described in this section require no configuration in RM Import.

### Creating a General Header and Footer File

A general header and footer file is used for all exported documents, unless a specific template overrides the default. For creating a template header and footer file see chapter ["Creating a Template Header and Footer File" on page 66](#).

**To create a new header and footer file:**

- 1 Create or open a Microsoft Word document that contains the header or footer. Save the Word document in HTML format.



**IMPORTANT!** You must set the file **Save as type** in Word to: **Web Page (\*.htm;\*.html)**.

Do **NOT** select "Single File Web Page (\*.mht;\*.mhtml)" or "Web Page, Filtered (\*.htm;\*.html)".

- 2 If it does not exist, create the directory *DataBase\_Name* in this directory  
`RM_Install\Common Tools #.#\tomcat\#.#\webapps\rtmBrowser\conf`



**NOTE** *Database\_Name* is identical with the database name from the login dialog.

- 3 If it does not exist, create the directory *Instance\_Name* inside the *DataBase\_Name* directory from [Step 2](#).



**NOTE** *Instance\_Name* is identical with the instance name from the login dialog.

- 4 If it does not exist, create the directory `publish templates` inside the *Instance\_Name* directory from [Step 3](#).
- 5 The save causes Word to create a subdirectory: *WordFileName\_files*. Copy the file `header.htm` from that directory to:  
`RM_Install\Common Tools #.#\tomcat\#.#\webapps\rtmBrowser\conf`  
`\Database_Name\Instance_Name`

## Creating a Template Header and Footer File

A template header and footer file resides in the same directory as the class template(s) created in chapter "[Creating Templates to Export Requirements](#)" on page 63 or alone. If you created a class template, you can start with step [Step 5](#).



**NOTE** These templates are not related to form templates (chapter "[Customizing Web Forms](#)" on page 50).

### To create a new header and footer file:

- 1 If it does not exist, create the directory *DataBase\_Name* in this directory  
`RM_Install\Common Tools #.#\tomcat\#.#\webapps\rtmBrowser\conf`



**NOTE** *Database\_Name* is identical with the database name from the login dialog.

- 2 If it does not exist, create the directory *Instance\_Name* inside the *DataBase\_Name* directory from [Step 1](#).



**NOTE** *Instance\_Name* is identical with the instance name from the login dialog.

- 3 If it does not exist, create the directory `publish templates` inside the `Instance_Name` directory from [Step 2](#).
- 4 Create the directory `TemplateDirectory` inside the `publish templates` directory from [Step 3](#). `TemplateDirectory` is the name you want displayed in the **Publish Requirement Template** list on the Format Document dialog.
- 5 Create or open a Microsoft Word document that contains the header or footer. Save the Word document in HTML format.



**IMPORTANT!** You must set the file **Save as type** in Word to: **Web Page (\*.htm;\*.html)**.

Do **NOT** select "Single File Web Page (\*.mht;\*.mhtml)" or "Web Page, Filtered (\*.htm;\*.html)".

- 6 In the same directory your HTML file is in, Word created a directory `WordFileName_files`. Copy the file `header.htm` from that directory to: `RM_Install\Common Tools \.#\tomcat\#\.#\webapps\rtmBrowser\conf \DataBase_Name\Instance_Name\publish templates\TemplateDirectory`



#### NOTE

- You must create the `Database_Name` and `Instance_Name` directories in the `conf` directory.
- A template header and footer file overrides a general header and footer file.

## Exporting a Document with File Attachments from a Separate Server

To be able to export documents with file attachments from Documents View in RM Browser, Microsoft Word must be installed on the server. This is not acceptable for some customers. To resolve this issue, a separate machine with Word installed on it can be used to redirect the exporting of a document. This machine also must have Dimensions RM installed on it and is referred to as a "publishing server." You configure the publishing server through a configuration file.



**NOTE** Both servers must have the same version of Dimensions RM installed on them, and both servers must point to the same Oracle instance.

#### To configure the publishing server:

Create a text file named `rm.cfg` in the following directory:

`RM_Install\Common Tools \.#\tomcat\#\.#\webapps\rtmBrowser\conf`

The format of the `rm.cfg` file follows:

```
[Document]
PublishServerURL=URL_of_publish_server
```

Database=*Database\_name*

For example: PublishServerURL=http://server/rtmBrowser

If any specified information cannot be found, the current server or current database is used.

## Customizing RM Browser Menus and Title Bars

You can use HTML and JavaScript to customize the menus and the Actions pane in RM Browser. You can change the following items:

- Menu text
- Tool tips
- Images
- Sequence
- Number of columns
- Title of the view in the title bar

You can also add extra menu items. The extra menu items can point to any HTTP address (for example, http://www.opentext.com) or execute JavaScript functions.

### Editing the Top Menu

The menus are defined in the file *RM\_Install\Common Tools* `#\tomcat\#\#\webapps\rtmBrowser\rm\frame\panels\top\toppanel.jsp`. You can define either buttons or menus. To edit `toppanel.jsp`, open it in a text editor, e.g. Notepad++.

#### **Defining a Button**

A button is defined by a `sct:largeButtonItem` tag

The `sct:largeButtonItem` tag must follow this format:

```
<sct:largeButtonItem href="javascript:customFunction()">Any HTML code</sct:largeButtonItem>
```

#### **Examples:**

##### Simple Button:

```
<sct:largeButtonItem href="javascript:customFunction()">  
  <span>Custom Button</span>  
</sct:largeButtonItem>
```

##### Button with Tool Tip:

```
<sct:largeButtonItem href="javascript:customFunction()" title="This is  
a custom button.">
```

```
<span>Custom Button</span>
</sct:largeButtonItem>
```

#### Button with Picture:

```
<sct:largeButtonItem href="javascript:customFunction()">
  
  <span>Custom Button</span>
</sct:largeButtonItem>
```

### **Defining a Menu**

A menu is defined by a `largeButtonItem` tag and contains one or several `subMenuItem` tags which define the menu entries.

The `sct:largeButtonItem` *should* follow this format:

```
<sct:largeButtonItem>HTML code and sct:subMenuItem tags
</sct:largeButtonItem>
```

Note that also for menus, you can define a tool tip by adding the `title` attribute to the `largeButtonItem`.

Each `subMenuItem` tag **must** follow this format:

```
<sct:subMenuItem href="javascript:customFunction()">Any HTML code
</sct:subMenuItem>
```

#### **On the subMenuItem tag, there are these restrictions:**

- There must be a `href` attribute.
- The `href` attribute must call a JavaScript function, e.g. `javascript:aFunction()`.
- The JavaScript function call in the `href` attribute **must** start with **javascript:**.
- No other attributes are allowed.



**CAUTION!** You **must** follow the `subMenuItem` format as described above, otherwise you cannot log in to Dimensions RM.

#### Simple Menu:

```
<sct:largeButtonItem>
  <span>Custom Menu</span>
  <sct:subMenu>
    <sct:subMenuItem href="javascript:customFunction()">Custom Entry
    </sct:subMenuItem>
    <sct:subMenuItem href="javascript>window.open('https://
www.opentext.com')">Open Text Homepage
    </sct:subMenuItem>
  </sct:subMenu>
</sct:largeButtonItem>
```

#### Menu with Tool Tips:

```
<sct:largeButtonItem>
  <span>Custom Menu</span>
```

```
<sct:subMenu>
  <sct:subMenuItem href="javascript:customFunction()">
    <span title="This is a custom entry.">Custom Entry</span>
  </sct:subMenuItem>
  <sct:subMenuItem href="javascript:window.open('https://
www.opentext.com')">
    <span title="Go to the Open Text homepage.">Open Text Homepage</
span>
  </sct:subMenuItem>
</sct:subMenu>
</sct:largeButtonItem>
```

#### Menu with Picture:

```
<sct:largeButtonItem>
  
  <span>Custom Menu</span>
  <sct:subMenu>
    <sct:subMenuItem href="javascript:customFunction()">Custom Entry
  </sct:subMenuItem>
    <sct:subMenuItem href="javascript:window.open('https://www.Open
Text.com')">Open Text Homepage
  </sct:subMenuItem>
  </sct:subMenu>
</sct:largeButtonItem>
```



**NOTE** After changing the `toppanel.jsp` file, you must restart the **Dimensions RM Common Tomcat** service.

## Editing the Action Pane of a View

The Action pane is defined by JSP files which are located in subdirectories of this path:

```
RM_Install\Common Tools \#.#\tomcat\#.#\webapps\rtmBrowser\rm
```

The following chapters describe how to modify the Action pane of the views. Since all JSP files are text files, you need to edit them in a text editor, e.g. Notepad.

### ***Editing the Action Pane of Home View***

Open `navigation\index.jsp` in a text editor, e.g. Notepad. The `index.jsp` file contains HTML and JSP tags.

#### **A group uses the following HTML tags:**

- DIV:** This tag defines the group.
- H2 and SPAN:** These tags define the headline.
- UL:** This tag defines a list of sub-items.
- LI:** This tag defines a single sub-item.
- DIV:** This tag defines a separator (horizontal line).

#### **Example:**

```

<c:set var="apGroupId" value="myCustomGroup"/>
<c:choose>
  <c:when test="\${actionPanelCollapseState[apGroupId] eq 'collapsed'}">
    <c:set var="css" value="collapsed"/>
  </c:when>
  <c:otherwise>
    <c:set var="css" value=""/>
  </c:otherwise>
</c:choose>
<div id="myCustomGroup" class='actionGroup ${css}'>
  <h2><span></span>My Custom Group</h2>
  <ul>
    <li id="btnCustom1" onclick="customFunction1()">Custom Entry 1</li>
    <div class="actionSeparator"></div>
    <li id="btnCustom2" onclick="customFunction2()" title="My Custom
Entry">Custom Entry 2</li>
  </ul>
</div>

```

The above example shows a group with 2 entries. Entry 2 makes use of the `title` attribute to show a tool tip. Both entries are separated by a horizontal line. When using this example in your own `index.jsp` file, you need to do the following:

**Change** `myCustomGroup` to a unique ID. Note that the `id` is used on `c:set` and `div`.

**Change** `My Custom Group` to a group title of your liking.

Change the **bold** HTML code to match your entries.



**NOTE** After changing the `index.jsp` file, you must restart the **Dimensions RM Common Tomcat** service.

### Editing the Action Pane of other Views

The following table shows the file name for each view.

| View         | File                         |
|--------------|------------------------------|
| Document     | documents\pagesupport.jsp    |
| My Work      | mywork\pagesupport.jsp       |
| Requirements | requirements\pagesupport.jsp |
| Traceability | traceability\pagesupport.jsp |

In `pagesupport.jsp` files, the groups are built by JavaScript. In your text editor, navigate to the line which contains `groups : [`. Then find the location where you want to insert your custom group.

#### A group uses the following elements:

**title:** The headline of the group.

**id:** The identifier of the group.

**collapsed:** References a variable which stores the collapsed/expanded state for the group.

**actions:** An array of entries within a group.

### An action uses the following elements:

**id:** The identifier of the group.

**action:** A JavaScript function which is executed when clicking the entry.

**message:** The HTML code which is used to display the entry in the group.

### Example:

```
{
  title : "My Custom Group",
  id : "myCustomGroup",
  collapsed : "${actionPanelCollapseState['myCustomGroup']}",
  actions : [
    { id : "newRTMDocumentMenu",
      action : "customFunction1()",
      message : "Custom Entry 1"
    },
    {},
    { id : "newRTMDocumentMenu",
      action : "customFunction2()",
      message : "<span title='My custom entry'>Custom Entry 2</span>"
    }
  ]
}
```

The above example shows a group with 2 entries. Entry 2 contains a **span** element with a **title** attribute to show a tool tip. Both entries are separated by a horizontal line, which is created by using `{}`. When using this example in your own `pagesupport.jsp` file, you need to do the following:

Change `myCustomGroup` to a unique ID. Note that the id is used on `id` and `collapsed`.

Change `My Custom Group` to a group title of your liking.

Change the **bold** JavaScript code to match your entries.



**CAUTION!** As groups and actions are arrays, they are separated with commas. The last group and the last action in a group **must not** have a comma after the closing curly brace `}`. If there are commas missing or additional commas in your JavaScript code, an error might occur when loading the view. Due to this error, the view may be incomplete or blank.



**NOTE** After changing the `pagesupport.jsp` file, you must restart the **Dimensions RM Common Tomcat** service.

## Changing the Default Settings of the RM Browser Text Editor

The "off-the-shelf" default font size of the RM Browser text editor is 10 points. An RM-specific setting in the `tinymce_custom.css` file changes this value to 12 points. The `tinymce_custom.css` file is located in the following directory:

```
<RM_Install\Common Tools \.#\tomcat\.#\webapps\rtmBrowser\css\tiny_mce
```



**NOTE** This setting applies to all instances hosted on the server.

For more information about using and customizing the text editor for RM Browser, please refer to the information about TinyMCE found on the Moxiecode Systems AB Web site.

## Customizing the Editable Grid

You can customize the look and behavior of the Editable Grid by using JavaScript. This is done by adding JavaScript to the following file on the RM Server:

```
Install_Dir\RM\rtmBrowser\rm\ext\Extensions.js
```

Initially, the `Extensions.js` file is empty. To add a customization, copy the appropriate JavaScript from the example file, paste it into `Extensions.js`, and then edit it to meet your specific needs. The example file is:

```
Install_Dir\RM\rtmBrowser\rm\ext\Extensions_example.js
```

Using JavaScript, you can achieve the following customizations of the Editable Grid:

**Remove the Add New Record** button from the Editable Grid toolbar.

**Hide specific columns** of the Editable Grid.

**Set specific columns** to be Read-Only.

**Set specific cells** to be Read-Only/Writable or Mandatory/Optional based upon the value of other cells in the row.

**Limit the items displayed** in a Pick List based upon the current value.

**Add buttons that can call other functions**, or external links, to populate a cell with data.

See the `Extensions_example.js` file for commented JavaScript examples of Editable Grid customizations.

## Configuring the Expansion and Collapse of RM Browser Sections

You can control whether sections on RM Browser Web pages use a scrolling mechanism to open and close or whether the sections open and close immediately when users click + or -. If you want the sections to scroll, you can specify the speed of the scrolling.

You configure this functionality using the `animationspeed` option in the `default.xml` file, which is located in the following location:

```
RM_Install\Common Tools #.#\tomcat\#.#\webapps\rtmBrowser\forms\common
```

You can also configure this functionality in custom Web forms.

By default, the scrolling speed is set to 0, and is set on the root form element in the `default.xml` file. When the `animationspeed` option is set on the root form element, it affects all sections. For an example of the option set on the root form element, see item 1 in the illustration under "[Template Layout](#)" on page 50.

To set different scrolling speeds for sections, set the `animationspeed` option on the individual section. For example:

```
<section type="standard" label="Standard Attributes" animationspeed="0"  
  />
```

To set no scrolling, set the `animationspeed` option to 0.

## Creating Custom Login Alert Pages for RM Browser

You can optionally require users to review and accept an alert page before displaying the RM Browser client. When you do this, users are presented with the page after entering their login credentials. Once they accept the page, the RM Browser client appears.

This is a useful way to communicate important new information to users before they use RM Browser. You can change this as often as needed.

### To configure a custom login alert page for RM Browser:

- 1 Create either or both of the following files on the RM server:

```
IN directory RM_Install\Common Tools  
#.#\tomcat\#.#\webapps\rtmBrowser
```

For most standard browsers, name the file: `warning.html`

If your users use Firefox create: `warning.txt`

- 2 Add the Alert text to these files.

If you used Microsoft Word to edit the HTML file save the file as a

Web Page, Filtered

to ensure that any Microsoft Office tags are removed. A true HTML editor is recommended.

# Customizing Headers and Footers of RM Browser Interface

You can customize the header and footer of the RM Browser interface. This allows administrators to add the company name, logo graphic, or a security banner to differentiate between test and production databases.

## To customize RM Browser headers and footers:

- 1 Make a backup copy of the web.xml file. It is on the server in the following location:  
`RM_Install\Common Tools \#\tomcat\#\#\webapps\rtmBrowser\WEB-INF`
- 2 Open the web.xml file in a text editor.
- 3 Locate the last "bean id" in the file. It begins :  
`<bean id="rmHeaderAndFooterText"`

- 4 Beneath this entry, there are two property tags:

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

Uncomment the property section you want to enable. To do this, remove the opening (`<!--`) and closing (`-->`) comment tags from around that property section.

- 5 In the relevant `<property name="URL">` statement, replace the placeholder *enter your link to custom header (or footer) here...* with the path to your header or footer file. This html file may be placed in the rtmBrowser folder.

For example:

If you have named your file `securityheader.html` and placed it in the folder:  
`RM_Install\Common Tools \#\tomcat\#\#\webapps\rtmBrowser`

Then, the URL property value would be:

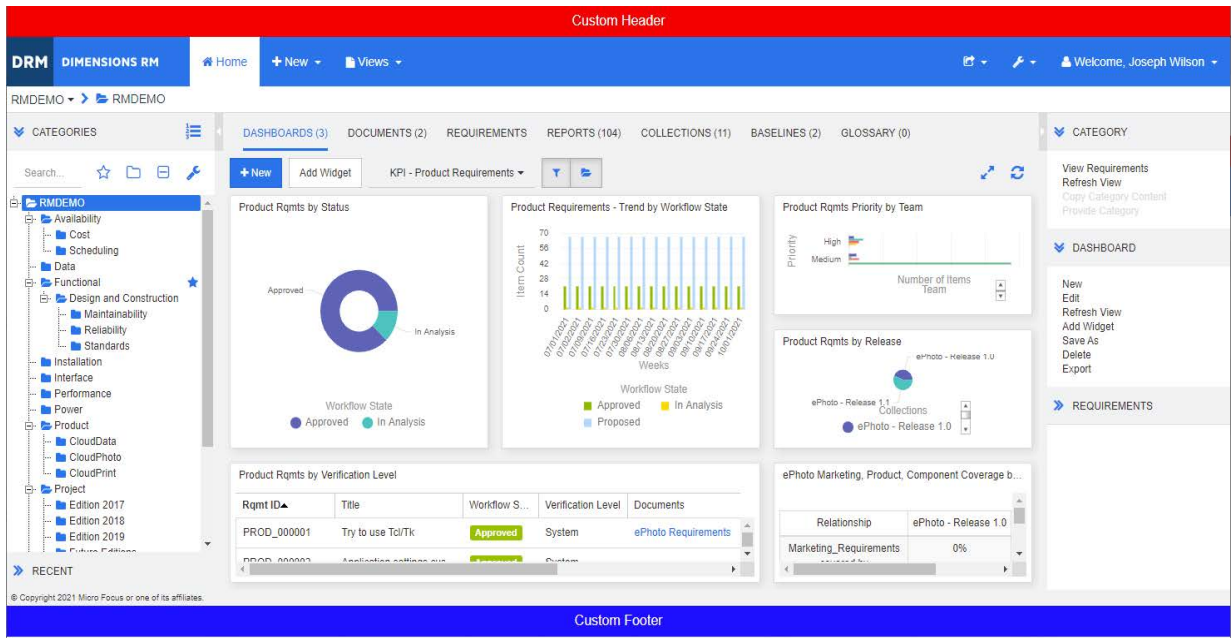
```
<property name="URL"><value>/rtmBrowser/html/securityheader.html</value></property>
```



**IMPORTANT!** Do not include quotation marks (") in the URL value.

- 6 Optionally, in the relevant `<property name="height">` statement, you can change the value (default: 20) with the desired height.
- 7 Save the file and restart the Dimensions RM Tomcat service (Dimensions RM Common Tomcat).

The following screen shot shows the location of the custom header and footer.



## Dashboard Export

Dashboards can be exported into PowerPoint presentations and PDF files. To allow this, a supported version of Microsoft® PowerPoint must be installed on the server running Dimensions RM.

### Using a Template

For creating the presentation, a template can be used. If you wish to use a template, it must be located in the `RM_Install\bin` directory and have the name `DashboardExport.pptx`.

When using a template, Dashboard Export will use the number of slides to identify the title slide and image slide.

If the template has only one slide, it is identified as image slide.

If the template has two or more slides, the first slide is identified as title slide; the second slide is identified as image slides. All subsequent slides will be ignored for processing, but remain in the final presentation.

The title box of the title or image slide supports the following placeholders:

Placeholder	Description
%NAME%	On the title slide, this placeholder is replaced by the dashboard name. On the image slide, this placeholder is replaced by the widget name.
%DATE%	On title or image slide, this placeholder is replaced by the current date with the format configured in the <code>DashboardExport.exe.config</code> file.

## Configuration

Dashboard export is configured by editing the `DashboardExport.exe.config` file, which is located in the `RM_Install\bin` directory.

The `DashboardExport.exe.config` file allows you to configure the following settings:

- **ImagePosition:** Defines the position of the image on the image. For the position, the horizontal (x) and vertical (y) value have to be specified in this format: `x, y`. The default `0, 130` means that the image will start at the leftmost position and 130 pixels from the top. Note that the x-position is ignored if the **CenterHorizontally** option is enabled.
- **AlwaysScaleImage:** If enabled, smaller images are scaled to match the maximum width or height (whichever is reached first). Allowed values are **True** or **False**. The default is **False** (disabled).
- **MaxImageSize:** Defines the maximum width and height of an image. The maximum image size must be specified in this format: **width, height**. When choosing the maximum image size, consider the size of the slide title. The default is **1280, 590**.
- **CenterHorizontally:** If enabled, images are centered horizontally. Allowed values are **True** or **False**. The default is **True** (enabled).
- **DateFormat:** Defines the date format used when using the **%DATE%** placeholder with the tile and/or image slide. All .NET date formats are supported. The default is **dd/MM/yyyy**. The following table provides some .NET date format strings:

Format	Description
d	Outputs the day with a single digit if possible (1-31).
dd	Outputs the day with two digits (01-31).
ddd	Outputs the abbreviated name of the day, e.g. Mon for Monday.
dddd	Outputs the full name of the day.
M	Outputs the month with a single digit if possible (1-12).
MM	Outputs the month with two digits (01-12).
MMM	Outputs the abbreviated name of the day, e.g. Jan for January.
MMMM	Outputs the full name of the month.
yyyy	Outputs the year with four digits.
h	Outputs the hour in 12-hour format with a single digit if possible (1-12).
hh	Outputs the hour in 12 hour format with two digits (01-12).
H	Outputs the hour in 24-hour format with a single digit if possible (0-23).
HH	Outputs the hour in 24hour format with two digits (00-23).
mm	Outputs the minutes with two digits.
ss	Outputs the seconds with two digits.
t	Outputs the first character of the AM/PM specifier.
tt	Outputs the complete AM/PM specifier.

## Command Line Parameters

DashboardExport.exe supports the following command line parameters:

**DashboardExport.exe /?|/help** Shows this help.

**DashboardExport.exe /showinfos** Shows information about the presentation used for export.

**DashboardExport.exe <filename>** Creates a presentation with the specified file name by using all PNG images in the same folder.

When using the **showinfos** parameter, DashboardExport.exe prints information about the template (if present) or the default presentation size (if no template is present) to the command prompt. This information (e.g. slide width and height in pixels) can be used to configure Dashboard Export.

# Chapter 3

---

## Agile

Creating Classes	80
Using Custom Classes	80
Creating Relationships	93
Enabling Agile	94
Products and Subcategories	94

## Creating Classes

In order to use Agile, several classes need to be added to the class definition.

**To add the classes follow these steps:**

- 1 Start the Class Definition tool as described in chapter "[Starting Class Definition](#)" on [page 270](#).
- 2 Right-click the background of your class definition.
- 3 From the shortcut menu, select **Add Class** and then **Product**.
- 4 Click into an empty space to place the new class.
- 5 Change the name to your liking, e.g. *Products* and press **Enter**.
- 6 Repeat steps 2-5 for the following template classes.



**NOTE** All classes below are optional. Depending on your use case, you may not need to create all classes.

- a Epics
  - b Features
  - c Releases
  - d Sprints
  - e Stories
  - f Tasks
- 7 Save the class definition.

## Using Custom Classes

To use custom classes, your classes must have attributes of certain types. You are free to name these classes and attributes as you like. The following chapters however use the default names.

## Epics Class

Attribute Name	Attribute Type	Options
<i>Assigned To</i>	User	<b>Attribute Mandatory:</b> No <b>Attribute Editable:</b> Yes <b>Force Unique Value:</b> No <b>Display For Entry:</b> Yes <b>Populate On Copy:</b> Yes <b>Populate On Create And Link:</b> Yes <b>Change Raises Suspicion:</b> No <b>All instance users:</b> Yes <b>All users from selected groups:</b> No <b>Specific users:</b> No <b>Allow multiple selections:</b> No
<i>Description</i>	Text	<b>Attribute Mandatory:</b> No <b>Attribute Editable:</b> Yes <b>Force Unique Value:</b> No <b>Display For Entry:</b> Yes <b>Populate On Copy:</b> Yes <b>Populate On Create And Link:</b> Yes <b>Change Raises Suspicion:</b> Yes <b>HTML Formatting:</b> Yes <b>Append Only:</b> No <b>Insert Newest First:</b> No
<i>Name</i>	Alphanumeric	<b>Attribute Mandatory:</b> Yes <b>Attribute Editable:</b> Yes <b>Force Unique Value:</b> No <b>Display For Entry:</b> Yes <b>Populate On Copy:</b> Yes <b>Populate On Create And Link:</b> Yes <b>Change Raises Suspicion:</b> Yes
<i>Priority</i>	List	<b>Attribute Mandatory:</b> No <b>Attribute Editable:</b> Yes <b>Force Unique Value:</b> No <b>Display For Entry:</b> Yes <b>Populate On Copy:</b> Yes <b>Populate On Create And Link:</b> Yes <b>Change Raises Suspicion:</b> Yes  <b>List Entries:</b> <ul style="list-style-type: none"> <li>■ High</li> <li>■ Medium</li> <li>■ Low</li> </ul> <b>Default Value:</b> Medium <b>Allow multiple selections:</b> No <b>Tag list:</b> No <b>Show as checkbox:</b> No

## Features Class

Attribute Name	Attribute Type	Options
<i>Assigned To</i>	User	<b>Attribute Mandatory:</b> No <b>Attribute Editable:</b> Yes <b>Force Unique Value:</b> No <b>Display For Entry:</b> Yes <b>Populate On Copy:</b> Yes <b>Populate On Create And Link:</b> Yes <b>Change Raises Suspicion:</b> No <b>All instance users:</b> Yes <b>All users from selected groups:</b> No <b>Specific users:</b> No <b>Allow multiple selections:</b> No
<i>Description</i>	Text	<b>Attribute Mandatory:</b> No <b>Attribute Editable:</b> Yes <b>Force Unique Value:</b> No <b>Display For Entry:</b> Yes <b>Populate On Copy:</b> Yes <b>Populate On Create And Link:</b> Yes <b>Change Raises Suspicion:</b> Yes <b>HTML Formatting:</b> Yes <b>Append Only:</b> No <b>Insert Newest First:</b> No
<i>Name</i>	Alphanumeric	<b>Attribute Mandatory:</b> Yes <b>Attribute Editable:</b> Yes <b>Force Unique Value:</b> No <b>Display For Entry:</b> Yes <b>Populate On Copy:</b> Yes <b>Populate On Create And Link:</b> Yes <b>Change Raises Suspicion:</b> Yes
<i>Priority</i>	List	<b>Attribute Mandatory:</b> No <b>Attribute Editable:</b> Yes <b>Force Unique Value:</b> No <b>Display For Entry:</b> Yes <b>Populate On Copy:</b> Yes <b>Populate On Create And Link:</b> Yes <b>Change Raises Suspicion:</b> Yes  <b>List Entries:</b> <ul style="list-style-type: none"> <li>• High</li> <li>• Medium</li> <li>• Low</li> </ul> <b>Default Value:</b> Medium <b>Allow multiple selections:</b> No <b>Tag list:</b> No <b>Show as checkbox:</b> No

## Products Class

Attribute Name	Attribute Type	Options
<i>Description</i>	Text	<b>Attribute Mandatory:</b> No <b>Attribute Editable:</b> Yes <b>Force Unique Value:</b> No <b>Display For Entry:</b> Yes <b>Populate On Copy:</b> Yes <b>Populate On Create And Link:</b> Yes <b>Change Raises Suspicion:</b> Yes <b>HTML Formatting:</b> Yes <b>Append Only:</b> No <b>Insert Newest First:</b> No
<i>Name</i>	Alphanumeric	<b>Attribute Mandatory:</b> Yes <b>Attribute Editable:</b> Yes <b>Force Unique Value:</b> No <b>Display For Entry:</b> Yes <b>Populate On Copy:</b> Yes <b>Populate On Create And Link:</b> Yes <b>Change Raises Suspicion:</b> Yes
<i>Short Name</i>	Alphanumeric	<b>Attribute Mandatory:</b> Yes <b>Attribute Editable:</b> Yes <b>Force Unique Value:</b> No <b>Display For Entry:</b> Yes <b>Populate On Copy:</b> Yes <b>Populate On Create And Link:</b> Yes <b>Change Raises Suspicion:</b> Yes
<i>Shown Classes</i>	Text	<b>Attribute Mandatory:</b> No <b>Attribute Editable:</b> Yes <b>Force Unique Value:</b> No <b>Display For Entry:</b> No <b>Populate On Copy:</b> Yes <b>Populate On Create And Link:</b> Yes <b>Change Raises Suspicion:</b> Yes <b>HTML Formatting:</b> No <b>Append Only:</b> No <b>Insert Newest First:</b> No
<i>Tabs</i>		<b>Attribute Mandatory:</b> No <b>Attribute Editable:</b> Yes <b>Force Unique Value:</b> No <b>Display For Entry:</b> No <b>Populate On Copy:</b> Yes <b>Populate On Create And Link:</b> Yes <b>Change Raises Suspicion:</b> Yes <b>HTML Formatting:</b> No <b>Append Only:</b> No <b>Insert Newest First:</b> No

## Releases Class

Attribute Name	Attribute Type	Options
<i>Capacity</i>	Numeric	<b>Attribute Mandatory:</b> No <b>Attribute Editable:</b> Yes <b>Force Unique Value:</b> No <b>Display For Entry:</b> Yes <b>Populate On Copy:</b> Yes <b>Populate On Create And Link:</b> Yes <b>Change Raises Suspicion:</b> Yes
<i>Description</i>	Text	<b>Attribute Mandatory:</b> No <b>Attribute Editable:</b> Yes <b>Force Unique Value:</b> No <b>Display For Entry:</b> Yes <b>Populate On Copy:</b> Yes <b>Populate On Create And Link:</b> Yes <b>Change Raises Suspicion:</b> Yes <b>HTML Formatting:</b> Yes <b>Append Only:</b> No <b>Insert Newest First:</b> No
<i>End Date</i>	Date	<b>Attribute Mandatory:</b> No <b>Attribute Editable:</b> Yes <b>Force Unique Value:</b> No <b>Display For Entry:</b> Yes <b>Populate On Copy:</b> Yes <b>Populate On Create And Link:</b> Yes <b>Change Raises Suspicion:</b> Yes <b>Display Format:</b> DD-MON-RRRR
<i>Name</i>	Alphanumeric	<b>Attribute Mandatory:</b> Yes <b>Attribute Editable:</b> Yes <b>Force Unique Value:</b> No <b>Display For Entry:</b> Yes <b>Populate On Copy:</b> Yes <b>Populate On Create And Link:</b> Yes <b>Change Raises Suspicion:</b> Yes
<i>Start Date</i>	Date	<b>Attribute Mandatory:</b> No <b>Attribute Editable:</b> Yes <b>Force Unique Value:</b> No <b>Display For Entry:</b> Yes <b>Populate On Copy:</b> Yes <b>Populate On Create And Link:</b> Yes <b>Change Raises Suspicion:</b> Yes <b>Display Format:</b> DD-MON-RRRR

---

Attribute Name	Attribute Type	Options
<i>Teams</i>	User	<b>Attribute Mandatory:</b> No <b>Attribute Editable:</b> Yes <b>Force Unique Value:</b> No <b>Display For Entry:</b> Yes <b>Populate On Copy:</b> Yes <b>Populate On Create And Link:</b> Yes <b>Change Raises Suspicion:</b> No <b>Allow multiple selections:</b> Yes <b>All instance users:</b> No <b>All users from selected groups:</b> No <b>Specific users:</b> No

## Sprints Class

Attribute Name	Attribute Type	Options
<i>Capacity</i>	Numeric	<b>Attribute Mandatory:</b> No <b>Attribute Editable:</b> Yes <b>Force Unique Value:</b> No <b>Display For Entry:</b> Yes <b>Populate On Copy:</b> Yes <b>Populate On Create And Link:</b> Yes <b>Change Raises Suspicion:</b> Yes
<i>End Date</i>	Date	<b>Attribute Mandatory:</b> No <b>Attribute Editable:</b> Yes <b>Force Unique Value:</b> No <b>Display For Entry:</b> Yes <b>Populate On Copy:</b> Yes <b>Populate On Create And Link:</b> Yes <b>Change Raises Suspicion:</b> Yes <b>Display Format:</b> DD-MON-RRRR
<i>Name</i>	Alphanumeric	<b>Attribute Mandatory:</b> Yes <b>Attribute Editable:</b> Yes <b>Force Unique Value:</b> No <b>Display For Entry:</b> Yes <b>Populate On Copy:</b> Yes <b>Populate On Create And Link:</b> Yes <b>Change Raises Suspicion:</b> Yes
<i>Sprint Goal</i>	Text	<b>Attribute Mandatory:</b> No <b>Attribute Editable:</b> Yes <b>Force Unique Value:</b> No <b>Display For Entry:</b> Yes <b>Populate On Copy:</b> Yes <b>Populate On Create And Link:</b> Yes <b>Change Raises Suspicion:</b> Yes <b>HTML Formatting:</b> Yes <b>Append Only:</b> No <b>Insert Newest First:</b> No
<i>Start Date</i>	Date	<b>Attribute Mandatory:</b> No <b>Attribute Editable:</b> Yes <b>Force Unique Value:</b> No <b>Display For Entry:</b> Yes <b>Populate On Copy:</b> Yes <b>Populate On Create And Link:</b> Yes <b>Change Raises Suspicion:</b> Yes <b>Display Format:</b> DD-MON-RRRR

---

Attribute Name	Attribute Type	Options
<i>Teams</i>	User	<b>Attribute Mandatory:</b> No <b>Attribute Editable:</b> Yes <b>Force Unique Value:</b> No <b>Display For Entry:</b> Yes <b>Populate On Copy:</b> Yes <b>Populate On Create And Link:</b> Yes <b>Change Raises Suspicion:</b> No <b>Allow multiple selections:</b> Yes <b>All instance users:</b> No <b>All users from selected groups:</b> No <b>Specific users:</b> No

## Stories Class

Attribute Name	Attribute Type	Options
<i>Acceptance Criteria</i>	Text	<b>Attribute Mandatory:</b> No <b>Attribute Editable:</b> Yes <b>Force Unique Value:</b> No <b>Display For Entry:</b> Yes <b>Populate On Copy:</b> Yes <b>Populate On Create And Link:</b> Yes <b>Change Raises Suspicion:</b> Yes <b>HTML Formatting:</b> No <b>Append Only:</b> No <b>Insert Newest First:</b> No
<i>Assigned To</i>	User	<b>Attribute Mandatory:</b> No <b>Attribute Editable:</b> Yes <b>Force Unique Value:</b> No <b>Display For Entry:</b> Yes <b>Populate On Copy:</b> Yes <b>Populate On Create And Link:</b> Yes <b>Change Raises Suspicion:</b> Yes <b>All instance users:</b> Yes <b>All users from selected groups:</b> No <b>Specific users:</b> No <b>Allow multiple selections:</b> No
<i>Color</i>	Alphanumeric	<b>Attribute Mandatory:</b> No <b>Attribute Editable:</b> Yes <b>Force Unique Value:</b> No <b>Display For Entry:</b> Yes <b>Populate On Copy:</b> Yes <b>Populate On Create And Link:</b> Yes <b>Change Raises Suspicion:</b> Yes
<i>Description</i>	Text	<b>Attribute Mandatory:</b> No <b>Attribute Editable:</b> Yes <b>Force Unique Value:</b> No <b>Display For Entry:</b> Yes <b>Populate On Copy:</b> Yes <b>Populate On Create And Link:</b> Yes <b>Change Raises Suspicion:</b> Yes <b>HTML Formatting:</b> Yes <b>Append Only:</b> No <b>Insert Newest First:</b> No
<i>Estimated Effort</i>	Numeric	<b>Attribute Mandatory:</b> No <b>Attribute Editable:</b> Yes <b>Force Unique Value:</b> No <b>Display For Entry:</b> Yes <b>Populate On Copy:</b> Yes <b>Populate On Create And Link:</b> Yes <b>Change Raises Suspicion:</b> Yes

Attribute Name	Attribute Type	Options
<i>Name</i>	Alphanumeric	<b>Attribute Mandatory:</b> Yes <b>Attribute Editable:</b> Yes <b>Force Unique Value:</b> No <b>Display For Entry:</b> Yes <b>Populate On Copy:</b> Yes <b>Populate On Create And Link:</b> Yes <b>Change Raises Suspicion:</b> Yes
<i>Planning Status</i>	List	<b>Attribute Mandatory:</b> Yes <b>Attribute Editable:</b> Yes <b>Force Unique Value:</b> No <b>Display For Entry:</b> Yes <b>Populate On Copy:</b> Yes <b>Populate On Create And Link:</b> Yes <b>Change Raises Suspicion:</b> Yes  <b>List Entries:</b> <ul style="list-style-type: none"> <li>• Elaborated</li> <li>• Pre-Planning</li> <li>• Sprint-Ready</li> </ul> <b>Default Value:</b> Elaborated <b>Allow multiple selections:</b> No <b>Tag list:</b> No <b>Show as checkbox:</b> No
<i>Priority</i>	List	<b>Attribute Mandatory:</b> No <b>Attribute Editable:</b> Yes <b>Force Unique Value:</b> No <b>Display For Entry:</b> Yes <b>Populate On Copy:</b> Yes <b>Populate On Create And Link:</b> Yes <b>Change Raises Suspicion:</b> Yes  <b>List Entries:</b> <ul style="list-style-type: none"> <li>• High</li> <li>• Medium</li> <li>• Low</li> </ul> <b>Default Value:</b> Low <b>Allow multiple selections:</b> No <b>Tag list:</b> No <b>Show as checkbox:</b> No

Attribute Name	Attribute Type	Options
<i>Ranking</i>	Numeric	<b>Attribute Mandatory:</b> No <b>Attribute Editable:</b> Yes <b>Force Unique Value:</b> No <b>Display For Entry:</b> Yes <b>Populate On Copy:</b> Yes <b>Populate On Create And Link:</b> Yes <b>Change Raises Suspicion:</b> Yes
<i>Remaining Effort</i>	Numeric	<b>Attribute Mandatory:</b> No <b>Attribute Editable:</b> Yes <b>Force Unique Value:</b> No <b>Display For Entry:</b> Yes <b>Populate On Copy:</b> Yes <b>Populate On Create And Link:</b> Yes <b>Change Raises Suspicion:</b> Yes
<i>Spent Effort</i>	Numeric	<b>Attribute Mandatory:</b> No <b>Attribute Editable:</b> Yes <b>Force Unique Value:</b> No <b>Display For Entry:</b> Yes <b>Populate On Copy:</b> No <b>Populate On Create And Link:</b> Yes <b>Change Raises Suspicion:</b> Yes
<i>Sprint Status</i>	List	<b>Attribute Mandatory:</b> Yes <b>Attribute Editable:</b> Yes <b>Force Unique Value:</b> No <b>Display For Entry:</b> Yes <b>Populate On Copy:</b> Yes <b>Populate On Create And Link:</b> Yes <b>Change Raises Suspicion:</b> Yes  <b>List Entries:</b> <ul style="list-style-type: none"> <li>• Not Started</li> <li>• In Development</li> <li>• In Test</li> <li>• In Review</li> <li>• Accepted</li> </ul> <b>Default Value:</b> Not Started <b>Allow multiple selections:</b> No <b>Tag list:</b> No <b>Show as checkbox:</b> No

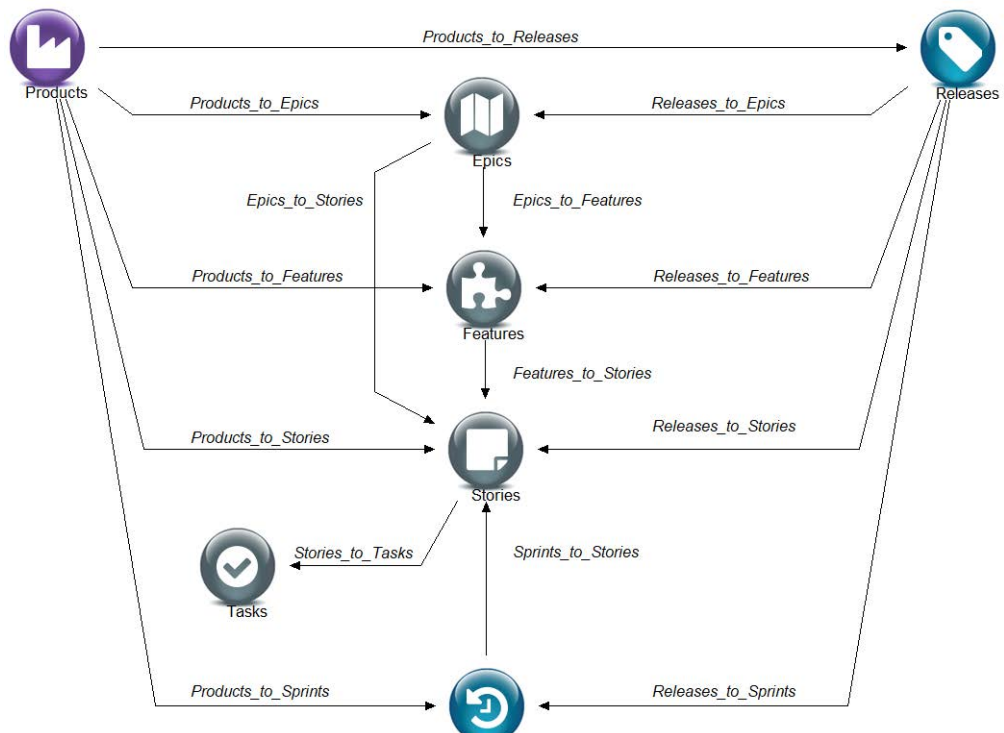
## Tasks Class

Attribute Name	Attribute Type	Options
<i>Assigned To</i>	User	<b>Attribute Mandatory:</b> No <b>Attribute Editable:</b> Yes <b>Force Unique Value:</b> No <b>Display For Entry:</b> Yes <b>Populate On Copy:</b> Yes <b>Populate On Create And Link:</b> Yes <b>Change Raises Suspicion:</b> Yes <b>All instance users:</b> Yes <b>All users from selected groups:</b> No <b>Specific users:</b> No <b>Allow multiple selections:</b> No
<i>Color</i>	Alphanumeric	<b>Attribute Mandatory:</b> No <b>Attribute Editable:</b> Yes <b>Force Unique Value:</b> No <b>Display For Entry:</b> Yes <b>Populate On Copy:</b> Yes <b>Populate On Create And Link:</b> Yes <b>Change Raises Suspicion:</b> Yes
<i>Description</i>	Text	<b>Attribute Mandatory:</b> No <b>Attribute Editable:</b> Yes <b>Force Unique Value:</b> No <b>Display For Entry:</b> Yes <b>Populate On Copy:</b> Yes <b>Populate On Create And Link:</b> Yes <b>Change Raises Suspicion:</b> Yes <b>HTML Formatting:</b> Yes
<i>Log</i>	Text	<b>Attribute Mandatory:</b> No <b>Attribute Editable:</b> Yes <b>Force Unique Value:</b> No <b>Display For Entry:</b> Yes <b>Populate On Copy:</b> Yes <b>Populate On Create And Link:</b> Yes <b>Change Raises Suspicion:</b> Yes <b>HTML Formatting:</b> Yes
<i>Name</i>	Alphanumeric	<b>Attribute Mandatory:</b> Yes <b>Attribute Editable:</b> Yes <b>Force Unique Value:</b> No <b>Display For Entry:</b> Yes <b>Populate On Copy:</b> Yes <b>Populate On Create And Link:</b> Yes <b>Change Raises Suspicion:</b> Yes

Attribute Name	Attribute Type	Options
<i>Priority</i>	List	<b>Attribute Mandatory:</b> No <b>Attribute Editable:</b> Yes <b>Force Unique Value:</b> No <b>Display For Entry:</b> Yes <b>Populate On Copy:</b> Yes <b>Populate On Create And Link:</b> Yes <b>Change Raises Suspicion:</b> Yes  <b>List Entries:</b> <ul style="list-style-type: none"><li>• High</li><li>• Medium</li><li>• Low</li></ul>
<i>Task Status</i>	List	<b>Attribute Mandatory:</b> Yes <b>Attribute Editable:</b> Yes <b>Force Unique Value:</b> No <b>Display For Entry:</b> Yes <b>Populate On Copy:</b> Yes <b>Populate On Create And Link:</b> Yes <b>Change Raises Suspicion:</b> Yes  <b>List Entries:</b> <ul style="list-style-type: none"><li>• To Do</li><li>• In Progress</li><li>• In Test</li><li>• Done</li></ul>

# Creating Relationships

After creating the classes, you need to create relationships between them.



## To create the relationships follow these steps:

- 1 Start the Class Definition tool as described in chapter "Starting Class Definition" on page 270.
- 2 Click the **Add Relationship** button .
- 3 Click the *Products* class.
- 4 Click the *Releases* class.
- 5 Specify a name for the relationship, e.g. *Products\_to\_Releases* and press **Enter**.
- 6 Repeat steps 2-5 for the following relationships:
  - a From *Epics* to *Features*.
  - b From *Epics* to *Stories*.
  - c From *Features* to *Stories*.
  - d From *Products* to *Epics*.
  - e From *Products* to *Features*.
  - f From *Products* to *Sprints*.
  - g From *Products* to *Stories*.
  - h From *Releases* to *Epics*.
  - i From *Releases* to *Features*.

- j** From *Releases* to *Sprints*.
  - k** From *Releases* to *Stories*.
  - l** From *Sprints* to *Stories*.
  - m** From *Stories* to *Tasks*.
- 7** Save the class definition.

## Enabling Agile

To enable Agile, see chapter *General Settings* in *Dimensions RM User's Guide*.

## Products and Subcategories

When using Agile, a category **Products** will be created automatically. This category can be used for storing products, as well as any other category. Note that for the **Products** category, no sub-categories should be created, because no products can be created in the subcategory. If you do not require the **Products** category, you can deactivate it by executing the steps described in chapter *Activating/Deactivating a Category* in the *Dimensions RM User's Guide*.

## Chapter 4

---

# Special Functions in Dimensions RM

About Special Functions	96
NLP Complexity Analysis - Implementation	96
NLP Similarity Analysis - Implementation	96
Configuration for Branching and Merging	97
Defining the Document Class	98
Defining the Glossary Class	99
Risk Management	99
Risk Management Class Definition	99
Risk Management Reporting	101
GitHub Integration	102
Chatbot Integration	103
Jira Integration	105
IP Restrictions for Groups	107
SSO and CAC Configuration	111
Redirecting Internal Web Service and REST Service Calls	125

## About Special Functions

Some functions in Dimensions RM are not enabled by default because special files and/or classes must be created to support them. However, we provide both tools and instructions for the System Administrator to implement these functions, should the team choose to use them.

The Implementation must be completed by the System Administrator, activation within each instance may be accomplished by the Instance Administrator, see "Using Special Functions" in the *Dimensions RM Browser User's Guide*.

Many customers implement special functions in a test environment, or a test instance, allowing users to try things out and to judge for themselves the benefit it will bring to their own process.

## NLP Complexity Analysis - Implementation

Natural Language Processing, as implemented in Dimensions RM, is based on the Flesch-Kincaid readability tests. Warnings or errors may be raised based on the complexity of a text attribute; what constitutes complexity can be decided by the users.

A pre-requisite to the inclusion of the complexity analysis is to download and incorporate the jar file, following the instructions below:

### To incorporate the jar file:

- 1 Download the file, `whelk-flesch-kincaid-0.1.11.jar` from the maven repository: [whelk-flesch-kincaid](#)
- 2 Stop the **Dimensions RM Common Tomcat** service.
- 3 Store the downloaded jar file in the Common Tomcat webapps lib folder, for example: `...\Dimensions 25.2\Common Tools 2.5.0.0\tomcat\10.1\webapps\rtmBrowser\WEB-INF\lib`.
- 4 Start the **Dimensions RM Common Tomcat** service.

Complexity analysis can be applied to selected classes within an instance. Once the System Administrator has made the function available, it can be activated and monitored by the Instance Administrator. See "Using Special Functions" in the *Dimensions RM Browser User's Guide*.

## NLP Similarity Analysis - Implementation

Natural Language processes design to analyze sentence similarity or semantic textual similarity is a measure of how similar two pieces of text are, or to what degree they express the same meaning.

To make **Similarity Analysis** available to Dimensions RM users, perform the following:

- 1 If you have implemented Complexity Analysis ("NLP Complexity Analysis - Implementation" on page 96) proceed to Step 3.

- 2 Download the file, `whelk-flesch-kincaid-0.1.11.jar` from the maven repository: [whelk-flesch-kincaid](#).
- 3 From <https://repo1.maven.org/maven2/org/tensorflow/tensorflow-core-api/0.2.0/> download the file **tensorflow-core-api-0.2.0-windows-x86\_64.jar**
- 4 From <https://tfhub.dev/google/universal-sentence-encoder/4> download the archive **universal-sentence-encoder\_4.tar.gz**. The downloaded file is about 935MB in size.
  - a Using 7zip, extract the downloaded archive; it will extract to a tar file.
  - b Use 7zip once again to extract the contents of the tar. The result will be 2 folders (assets and variables) and the model: `saved_model.pb` as shown below.
- 5 Stop the **Dimensions RM Common Tomcat** service.
- 6 If not already present, please copy the **whelk-flesch-kincaid-0.1.11.jar** file into the Common Tomcat webapps lib folder, for example: `...\Dimensions 25.2\Common Tools 2.5.0.0\tomcat\10.1\webapps\rtmBrowser\WEB-INF\lib`.
- 7 Copy the file **tensorflow-core-api-0.2.0-windows-x86\_64.jar** into the Common Tomcat webapps lib folder, for example: `...\Dimensions 25.2\Common Tools 2.5.0.0\tomcat\10.1\webapps\rtmBrowser\WEB-INF\lib`.
- 8 In the `webapps\rtmBrowser` folder, create a new folder named: **use**. For example: `...\Common Tools 2.5.0.0\tomcat\10.1\webapps\rtmBrowser\use`
- 9 Into the new folder place the content extracted from the tar file:

> Common Tools 1.8.6.0 > tomcat > 9.0 > webapps > rtmBrowser > use

Name	Date modified	Type	Size
assets	11/26/2019 3:50 AM	File folder	
variables	2/13/2023 6:24 PM	File folder	
saved_model.pb	11/26/2019 3:50 AM	PB File	8,032 KB

- 10 Start the **Dimensions RM Common Tomcat** service.

Similarity analysis enabled and monitored by the Instance Administrator. See "Using Special Functions" in the *Dimensions RM Browser User's Guide*.

## Configuration for Branching and Merging

The document management and category features of RM simplify the management of multiple releases, or custom releases. New requirements, for example, can be assigned to a planned new release, e.g. 3.2.2, of a product while the set of requirements still under development can be safely controlled in release 3.2.1 by managing requirements in separate documents with reasonable naming conventions.

However, there are organizations providing functionality for printers, cars and planes that require a permanent "Branching". Organizations building guidance systems, software and hardware to open car doors for a variety of models and power engines using components that must be modified for a targeted

manufacturer. In such organizations, there is no intent to merge all variants – but there is a need to maintain a common set of requirements as well as to maintain and track variant streams. It should also be possible to compare variants and to share or to merge back into the core.

Dimensions RM supports branching through the use of a Product class, with associated Project classes. Product and Project are class types, the names assigned to these class types are based on the local lexicon.

The product and project classes may be defined by the System Administrator, or by the Instance Administrator once the schema has been defined. To add the classes using RM Manage, follow these steps:

1 Start the Class Definition tool as described in chapter ["Starting Class Definition"](#) on page 270.

**2 Add the Product class:**




**NOTE** If you are using Agile and created the **Product** class as part of the Agile configuration, continue with step 3.

- a Right-click the background of your class definition.
- b From the shortcut menu, select **Add Class** and then **Product**.
- c Click into an empty space to place the new class.
- d Change the name to your liking, e.g. *Product* and press **Enter**.

**3 Add the Project class:**

- a Right-click the background of your class definition.
- b From the shortcut menu, select **Add Class** and then **Project**.
- c Click into an empty space to place the new class.
- d Change the name to your liking, e.g. *Project* and press **Enter**.


4 Save the class definition by clicking  in the toolbar.

## Defining the Document Class

In order to use documents, a Chapter class must be added to the class definition.

**To add the Chapter class, follow these steps:**


- 1 Start the Class Definition tool as described in chapter ["Starting Class Definition"](#) on page 270.
- 2 Right-click the background of your class definition.
- 3 From the shortcut menu, select **Add Class** and then **Chapter**.
- 4 Click into an empty space to place the new class.
- 5 Change the name to your liking, e.g. *Chapter* and press **Enter**.
- 6 To configure if users can hide chapter numbers:

- a Double-click the *Chapter* class. This opens the **Definition of class** dialog.
  - b Double-click the **Hide Chapter Number** attribute. This opens the **Definition of attribute** dialog.
  - c To allow users to hide chapter numbers, the **Display For Entry** option must be selected. If users should not be allowed to hide chapter numbers, clear the **Display For Entry** option.
  - d Click **OK** to close the **Definition of attribute** dialog.
  - e Click **OK** to close the **Definition of class** dialog.
- 7 Save the class definition by clicking  in the toolbar.

## Defining the Glossary Class

In order to use a glossary, a Glossary class needs to be added to the class definition.

**To add the Glossary class, follow these steps:**

- 1 Start the Class Definition tool as described in chapter "[Starting Class Definition](#)" on [page 270](#).
- 2 Right-click the background of your class definition.
- 3 From the shortcut menu, select **Add Class** and then **Glossary**.
- 4 Click into an empty space to place the new class.
- 5 Change the name to your liking, e.g. *Glossary* and press **Enter**.
- 6 Save the class definition by clicking  in the toolbar.

## Risk Management

### ***Risk Management Class Definition***

Risk Management is a core discipline in Business Analysis and Systems Engineering whose function is to identify, analyze, and evaluate risks that could negatively impact the product outcome.

To implement Risk Management a new class of type: **Risk** is now available in Schema Definition. As with all class types defined for use within the solution, this class has been populated with suggested attributes, which may be modified by the customer.

**To create the class, follow these steps:**

- 1 Start **RM Manage** (you might also use **Schema Definition** in the Browser}.
- 2 Login and expand the database in which your instance resides.
- 3 Right-click your instance and select **Define Instance Schema** in the shortcut menu.

- 4 In the Class Definition dialog, right-click on a free space and select **Add Class | Risk** from the shortcut menu.
- 5 Click on a free space to place the new class.
- 6 Change the name to your liking, e.g. Risk\_Mgt.
- 7 Save the class definition.

The default Risk class contains the following User Defined Attributes, any or all of which may be modified (see ["Defining an Attribute" on page 295](#)). However, you may want to test the functionality, which includes a **Risk** tab on the **Home View**.

Attribute Name	Description
Action Taken	Text attribute that describes the action taken to mitigate the risk.
Description	Text attribute that describes the risk.
Mitigation Strategy	Text attribute that provides a summary of the risk mitigation strategy.
Occurrence Rating (Initial)	Numeric attribute identifying the initial occurrence rating of the risk. 1 - Improbable 2 - Possible 3 - Probable
Occurrence Rating (Final)	Numeric attribute identifying the Final occurrence rating of the risk. 1 - Improbable 2 - Possible 3 - Probable
Potential Causes	Text attribute listing potential faults causing a failure
Potential Effects	Text attribute listing potential effects of failure
Reason for Change	Standard text attribute that identifies the reason for a proposed object change. If change proposals will not be used, it is best to hide this attribute from view. By unchecking all boxes in the <b>Core</b> tab (see <a href="#">"Core Tab" on page 296</a> ), the attribute will not be displayed for entry nor appear, by default, on the edit requirement form.
Recommended Action	Text attribute identifying remedial action, e.g. addition of safety feature(s), recommended to reduce the Risk Priority Number (RPN).
Responsible	User attribute identifying the responsible user or group responsible for mitigation.
Severity Rating - Final	Numeric attribute that identifies the final severity rating of the risk. 1 - Acceptable 2 - Tolerable 3 - Undesirable 4 - Intolerable

Attribute Name	Description
Severity Rating - Initial	Numeric attribute that identifies the final severity rating of the risk. 1 - Acceptable 2 - Tolerable 3 - Undesirable 4 - Intolerable
Title	Alphanumeric attribute that contains the title or summary of the risk.

### Risk Management Reporting

In addition to all standard reporting facilities, a **Risks** tab may be added to the Home View. The tab is defined in **Instance Settings**, using the attribute names defined in class definition. This tab was designed to use color coding to calculate and display the current risk threat.

Title	Severity Rating - Initial	Occurrence Rating - Initial	Severity Rating - Final	Occurrence Rating - Final	Risk Priority - Initial	Risk Priority - Final
Performance goals...	3	3	2	2	High	Medium
SLA not reached	3	2	2	1	High	Medium
Data loss in integr...	4	2	4	2	Extreme	Extreme
Increasing round-tr...	2	2	2	3	Medium	High

To define and activate the Risks tab:

- 1 Administration-->Instance Settings --> Risks
- 2 Name the levels of risk impact and use the color bar to reflect those levels. The icons to the right allow the deletion of a row, or the re-ordering of the display.

Name	Color	Description
Low	<span style="color: green;">■</span>	Low probability with little or no effect
Medium	<span style="color: yellow;">■</span>	Some annoyance, but not critical to the operation
High	<span style="color: orange;">■</span>	
Extreme	<span style="color: red;">■</span>	

Severity: Acceptable  
Little to no effect on event

Occurrence:

Color picker: R: 241, G: 255, B: 51

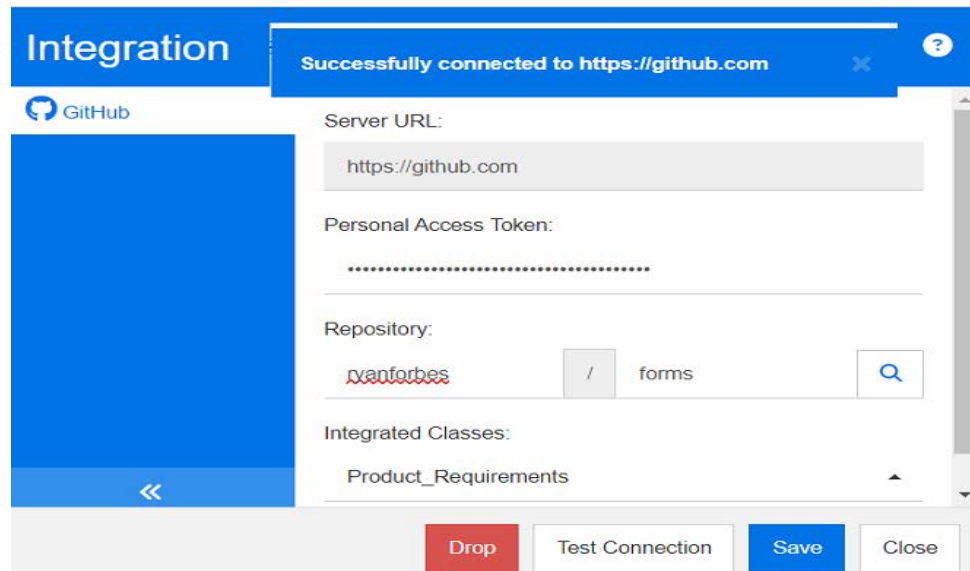
- The matrix calculation is based on the content of the Occurrence and Severity Initial and the Occurrence and Severity Final. Names and Descriptions may be modified.

Severity:	Acceptable	Tolerable	Undesirable	Intolerable
	Little to no effect on event	Effects are felt, but not critical to outcome	Serious impact to the course of action and outcome	Could result in disaster
Occurrence:				
Improbable Risk is unlikely to occur	Low	Medium	Medium	High
Possible Risk will likely occur	Low	Medium	High	Extreme
Probable Risk will occur	Medium	High	High	Extreme

## GitHub Integration

The GitHub integration dialog can be used to connect Dimensions RM to the organization's GitHub repository.

Enter the Personal Access Token (classic), the repository information and the Classes selected for integration. Use the Test Connection button to validate your selection.



# Chatbot Integration

The Rasa chatbot allows users to ask questions in natural language and receive instructions how to complete their tasks.

For integrating the Rasa chatbot with Dimensions RM, you can choose to install manually ("Chatbot Installation" on page 103) or by using a Docker image ("Docker Image Installation" on page 104).

The Rasa chatbot can be installed on a separate server, or on the same server as Dimensions RM.

## Chatbot Installation

### Before you continue

The following steps assume that you have installed the Rasa chatbot on your Dimensions RM server. For further details on how to install the chatbot, see

<https://rasa.com/docs/rasa/2.x/installation>.

### To install the chatbot, execute these steps:

- 1 Install the Rasa server following the official installation instructions at <https://rasa.com/docs/rasa/2.x/installation>.
- 2 Unarchive the ChatBot.zip file to your preferred location, e.g. *C:\temp*. The ChatBot.zip file contains chatbot models to be used with Dimensions RM and can be found on your Dimensions RM server under *RM\_INSTALL\RM\tutorial\ChatBot*, e.g. *C:\Program Files\Open Text\Dimensions 25.2\RM\tutorial\ChatBot*.
- 3 Open a command prompt and change to the directory to which you unarchived the ChatBot.zip file, e.g. *C:\temp*.
- 4 Type the following command and press **Enter**: `notepad endpoints.xml`.
- 5 Locate the following lines:  

```
action_endpoint:  
  url: "http://<HOST>:<PORT>/rtmBrowser/rest/rasa/webhook"
```
- 6 Change the marked sections to match your environment:
  - **http**: Change to **https** if you configured Tomcat to use secure connections.
  - **<HOST>**: Change to your server name or to the IP address of your Tomcat installation.
  - **<PORT>**: Change to the port of your Tomcat installation.
- 7 Save the file and close Notepad.
- 8 Type the following command and press **Enter**:

```
rasa run --enable-api --cors "*" --port 5005
```

Change the port number as desired.

Remember to **take a note** of the port number, because you will need during the configuration.

- 9 Continue with the steps described in chapter ["Configuring the Chatbot" on page 105](#).

## Docker Image Installation

### Before you continue

You must insure that the following is installed:

- Docker
- docker-compose

### To install the chatbot, execute these steps:

- 1 Extract the contents of ChatBot.zip to your preferred location, e.g. *C:\temp*. The ChatBot.zip file contains chatbot models to be used with Dimensions RM and can be found on your Dimensions RM server under *RM\_INSTALL\RM\tutorial\ChatBot*, e.g. *C:\Program Files\Open Text\Dimensions 25.2\RM\tutorial\ChatBot*
- 2 Open a command prompt and change to the directory to which you unarchived the ChatBot.zip file, e.g. *C:\temp*.
- 3 Type the following command and press **Enter**: `notepad endpoints.yml`.
- 4 Locate the following lines:  

```
action_endpoint:  
    url: "http://192.168.2.17:8080/rtmBrowser/rest/rasa/webhook"
```
- 5 Change the marked sections to match your environment:
  - **http**: Change to **https** if you configured Tomcat to use secure connections.
  - **192.168.2.17**: Change to your server name or to the IP address of your Tomcat installation.
  - **8080**: Change to the port of your Tomcat installation.
- 6 Save the file and close Notepad.
- 7 By default, the chatbot has been configured to use port 5005. If you want to change the port, do the following:
  - a Type the following command and press **Enter**: `notepad docker-compose.yml`.
  - b Locate the following lines:  

```
ports:  
- 5005:5005
```
  - c Change the marked number to the desired port number, e.g. `- 5005:6006`  
Remember to **take a note** of the port number, because you will need during the configuration.
  - d Save the file and close Notepad.
- 8 Type the following command and press **Enter**:  
`docker docker-compose up -d`
- 9 Continue with the steps described in chapter ["Configuring the Chatbot" on page 105](#).

---

## Configuring the Chatbot

### Before you continue

You must insure that the chatbot is installed either by executing the steps from chapter "Chatbot Installation" on page 103, or from chapter "Docker Image Installation" on page 104.

### To configure the chatbot, execute these steps:

- 1 Stop Services:
  - a **Dimensions RM Common Tomcat**
  - b **Dimensions RM Pool Manager**
- 2 In Windows Explorer, navigate to *RM\_INSTALL\RM\conf*, e.g. *C:\Program Files\Open Text\Dimensions 25.2\RM\conf*.
- 3 Open the file *chatbot.properties* with Notepad or another plain text editor.
- 4 For the *enabled* setting, change the value to **true**, so the line reads *enabled=true*.
- 5 For the *host* setting, change the value to your server name or IP address your Rasa server is running on, e.g. *host=myrasaserver*.
- 6 If you changed the port during the installation, change the value for the *port* setting to the new port, e.g. *port=6006*.
- 7 Save the file.
- 8 Start Services:
  - a **Dimensions RM Common Tomcat**
  - b **Dimensions RM Pool Manager**

## Jira Integration

The Dimensions RM / Jira Integration is implemented using Open Text MF Connect.

MF Connect is a data synchronization technology providing data and relationship synchronization between products across the software development / DevOps lifecycle.

Instructions for using MF Connect can be found at:

<http://admhelp.microfocus.com/connect/>

In conjunction with the MF Connect implementation and installation guidelines, the following are sample Data Source files from an existing RM / Jira integration:

PROPERTIES		TYPES	RELATIONSHIPS
<input type="button" value="Cancel"/> <input checked="" type="button" value="Save"/> <input checked="" type="button" value="Save/Clear Water Marks"/> <input type="button" value="Next"/> <input type="button" value="View ReadMe"/>			
Property	Value		
URL	https://dimrm.atlassian.net/		
Authorization Mechanism	User And Password (no OAuth2)		
HTTPTimeout, millis	300000		
Inject Comment Header Into Comm...	true		
User Name	qa.julia.combs@gmail.com		
Password	*****		
Disable Use of Authentication Cooki...	false		
Sample Project Key with Name	KAN:My Kanban Project		
Sample Project with Board	KAN:KAN board		
Default Link Type	blocks		
Types (leave blank for all)			
Force Properties to be Writable (<ty...			
Use Wiki to Store Rich Text	true		
Disable Optimized Field Fetch	true		
Time tracking precision	Minute		
Include comments since date (yyyy-...			

Figure 4-1. Sample Dimensions RM Data Source

PROPERTIES		TYPES	RELATIONSHIPS
<input type="button" value="Cancel"/> <input checked="" type="button" value="Save"/> <input checked="" type="button" value="Save/Clear Water Marks"/> <input type="button" value="Next"/> <input type="button" value="View ReadMe"/>			
Property	Value		
URL	https://dimrm.atlassian.net/		
Authorization Mechanism	User And Password (no OAuth2)		
HTTPTimeout, millis	300000		
Inject Comment Header Into Comm...	true		
User Name	qa.julia.combs@gmail.com		
Password	*****		
Disable Use of Authentication Cooki...	false		
Sample Project Key with Name	KAN:My Kanban Project		
Sample Project with Board	KAN:KAN board		
Default Link Type	blocks		
Types (leave blank for all)			
Force Properties to be Writable (<ty...			
Use Wiki to Store Rich Text	true		
Disable Optimized Field Fetch	true		
Time tracking precision	Minute		
Include comments since date (yyyy-...			

Figure 4-2. Sample Jira Data Source

# IP Restrictions for Groups

Restricting logins to originate from certain IP addresses is a security feature that makes attacks on the Dimensions RM more difficult. For using this feature, you have to send SQL commands to the server.



## NOTE

- **Oracle:**
  - All SQL examples will use SQLPlus
  - SQL commands always end with a semicolon
- **MS SQL Server:** All SQL examples will use SQL Server Management Studio
- **IPv6:** IPv6 is supported. Note that IPv6 addresses are case sensitive.

## In general, you should execute the following procedure:

- 1 Retrieve group Infos (see chapter ["Retrieving Group Infos" on page 107](#)). Query shows group ID, group name and if the IP restrictions have been enabled for that group.  
If the FILTER\_BY\_IP attribute has a value of 0, restrictions are disabled.  
If the FILTER\_BY\_IP attribute has a value of 1, restrictions are enabled.
- 2 Enable IP restrictions for group if check showed it is not enabled (see chapter ["Enabling IP Restrictions" on page 108](#))
- 3 Restrict groups by IP addresses (see chapter ["Restricting Groups by IP Addresses" on page 110](#))

## Retrieving Group Infos

### *Retrieving Group Infos with Oracle*

- 1 Open a command prompt.
- 2 Type sqlplus and press **Enter**.
- 3 Login with user icadmin for your database, e.g. icadmin@rtm.
- 4 Type the password for the ICADMIN user and press **Enter**. Note that SQLPlus does not show any characters for that password.
- 5 Type the following command and press **Enter**:  

```
select GROUP_ID, NAME, FILTER_BY_IP from adm_groups order by NAME;
```

### **Retrieving Group Infos with MS SQL Server**

- 1 Start **MS SQL Server Management Studio**.
- 2 Select your server instance.
- 3 Login with user sa.
- 4 Type the password for the sa user and click **Connect**.
- 5 Click **New Query**. This opens a new SQL query sheet.
- 6 Type the following command:  

```
select GROUP_ID, NAME, FILTER_BY_IP from  
<DATABASE>.ICADMIN.adm_groups order by NAME
```



**IMPORTANT!** Replace <DATABASE> with the actual database, e.g. RTM.

- 7 Click **Execute**.

## **Enabling IP Restrictions**

### **Enabling IP Restrictions with Oracle**

- 1 Open a command prompt.
- 2 Type sqlplus and press **Enter**.
- 3 Login with user icadmin for your database, e.g. icadmin@rtm.
- 4 Type the password for the ICADMIN user and press **Enter**. Note that SQLPlus does not show any characters for that password.
- 5 Type the following command and press **Enter**:  

```
update adm_groups set FILTER_BY_IP=1 where GROUP_ID=<GROUP_ID>;
```



**IMPORTANT!** Replace <GROUP\_ID> with the actual group ID (which you retrieved in chapter "Retrieving Group Infos with Oracle" on page 107).

### **Enabling IP Restrictions with MS SQL Server**

- 1 Start **MS SQL Server Management Studio**.
- 2 Select your server instance.
- 3 Login with user sa.
- 4 Type the password for the sa user and click **Connect**.
- 5 Click **New Query**. This opens a new SQL query sheet.

- 6 Type the following command:  

```
update <DATABASE>.ICADMIN.adm_groups set FILTER_BY_IP=1 where
GROUP_ID=<GROUP_ID>
```

**IMPORTANT!**

- Replace <DATABASE> with the actual database, e.g. RTM
- Replace <GROUP\_ID> with the actual group ID (which you retrieved in chapter "Retrieving Group Infos with MS SQL Server" on page 108)

- 7 Click **Execute**.

## Disabling IP Restrictions

### *Disabling IP Restrictions with Oracle*

- 1 Open a command prompt.
- 2 Type sqlplus and press **Enter**.
- 3 Login with user icadmin for your database, e.g. icadmin@rtm.
- 4 Type the password for the ICADMIN user and press **Enter**. Note that SQLPlus does not show any characters for that password.
- 5 Type the following command and press **Enter**:  

```
update adm_groups set FILTER_BY_IP=0 where GROUP_ID=<GROUP_ID>;
```



**IMPORTANT!** Replace <GROUP\_ID> with the actual group ID (which you retrieved in chapter "Retrieving Group Infos with Oracle" on page 107).

### *Disabling IP Restrictions with MS SQL Server*

- 1 Start **MS SQL Server Management Studio**.
- 2 Select your server instance.
- 3 Login with user sa.
- 4 Type the password for the sa user and click **Connect**.
- 5 Click **New Query**. This opens a new SQL query sheet.
- 6 Type the following command:  

```
update <DATABASE>.ICADMIN.adm_groups set FILTER_BY_IP=0 where
GROUP_ID=<GROUP_ID>
```

**IMPORTANT!**

- Replace <DATABASE> with the actual database, e.g. RTM
- Replace <GROUP\_ID> with the actual group ID (which you retrieved in chapter "Retrieving Group Infos with MS SQL Server" on page 108)

- 7 Click **Execute**.

## Restricting Groups by IP Addresses

### *Restricting Groups by IP Addresses with Oracle*

- 1 Open a command prompt.
- 2 Type sqlplus and press **Enter**.
- 3 Login with user icadmin for your database, e.g. icadmin@rtm.
- 4 Type the password for the ICADMIN user and press **Enter**. Note that SQLPlus does not show any characters for that password.
- 5 Type the following command and press **Enter**:  

```
insert into adm_groups_ip(GROUP_ID, IP_ADDRESS)
VALUES(<GROUP_ID>, '<IP_ADDRESS>');
```



#### **IMPORTANT!**

- Replace `<GROUP_ID>` with the actual group ID (which you retrieved in chapter ["Retrieving Group Infos with Oracle" on page 107](#))
- Replace `<IP_ADDRESS>` with the IP address which you want to allow access

### *Restricting Groups by IP Addresses with MS SQL Server*

- 1 Start **MS SQL Server Management Studio**.
- 2 Select your server instance.
- 3 Login with user sa.
- 4 Type the password for the sa user and click **Connect**.
- 5 Click **New Query**. This opens a new SQL query sheet.
- 6 Type the following command:  

```
insert into <DATABASE>.ICADMIN.adm_groups_ip(GROUP_ID, IP_ADDRESS)
VALUES(<GROUP_ID>, '<IP_ADDRESS>')
```



#### **IMPORTANT!**

- Replace `<DATABASE>` with the actual database, e.g. RTM
- Replace `<GROUP_ID>` with the actual group ID (which you retrieved in chapter ["Retrieving Group Infos with MS SQL Server" on page 108](#))
- Replace `<IP_ADDRESS>` with the IP address which you want to allow access

## Retrieving IP Addresses of Logged In Users

The following steps describe how to retrieve the IP addresses of logged in users. This allows you to verify the groups of those users and add their IP addresses as described in chapter "Restricting Groups by IP Addresses" on page 110.

### Retrieving IP Addresses of Logged In Users with Oracle

- 1 Open a command prompt.
- 2 Type `sqlplus` and press **Enter**.
- 3 Login with user `<RM_INSTANCE>` for your database, e.g. `rmdemo@rtm`.
- 4 Type the password for the RM instance and press **Enter**. Note that SQLPlus does not show any characters for that password.
- 5 Type the following command and press **Enter**:  

```
select USER_NAME, LOCATION, LAST_ACTIVE_TIME from user_sessions
order by USER_NAME, LAST_ACTIVE_TIME DESC;
```

### Retrieving IP Addresses of Logged In Users with MS SQL Server

- 1 Start **MS SQL Server Management Studio**.
- 2 Select your server instance.
- 3 Login with user `sa`.
- 4 Type the password for the `sa` user and click **Connect**.
- 5 Click **New Query**. This opens a new SQL query sheet.
- 6 Type the following command:  

```
select USER_NAME, LOCATION, LAST_ACTIVE_TIME from
<DATABASE>.<RM_INSTANCE>.user_sessions order by USER_NAME,
LAST_ACTIVE_TIME DESC
```



#### IMPORTANT!

- Replace `<DATABASE>` with the actual database, e.g. `RTM`
- Replace `<RM_INSTANCE>` with name of your Dimensions RM instance.

## SSO and CAC Configuration

The 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, 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 112](#), ["Exporting a Certificate from the STS Server" on page 113](#) and ["Adding a Certificate for RM Server to the STS Keystore" on page 113](#).

- 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 **Dimensions RM 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 433](#).

- 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 437 or "Exporting the STS Certificate from SBM Configurator" on page 438.



**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\Open Text\Dimensions 25.2\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 120.

**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 432 or "Exporting Certificates to CER Format from IIS" on page 433.
- 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 [Product Name Short No Marks] directory, e.g. *C:\Program Files\Open Text\Dimensions 25.2 (13)*.
- Replace *###.#* with the Common Tools version number, e.g. 2.3.0.0.
- Replace *##* with the Java version number, e.g. 11.0.

The complete set command should resemble the following:

```
set path=%path%;"RM_Install\Common Tools 2.3.0.0\jre\11.0\bin"
```

- 4 Navigate to the location of the truststore, which is at *SBM\_Install\Common\Tomcat x.x\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):

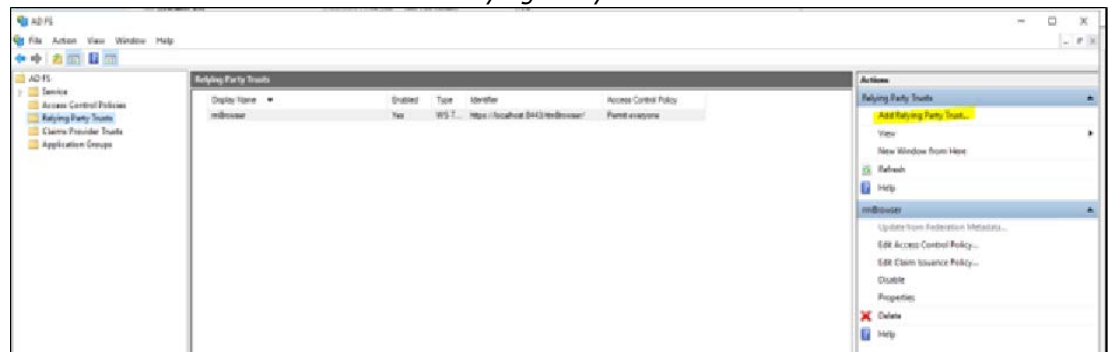
```
keytool -import -trustcacerts -keystore truststore.jks
-alias rmserver -file "C:\My Certificates\MyCert.cer"
```

## Configuring SSO with AD FS

### Part 1: Initiate Configuration Using AD FS Management Application

This section of the configuration addresses the initial configuration using the Active Directory Federation Services (AD FS) Management Application.

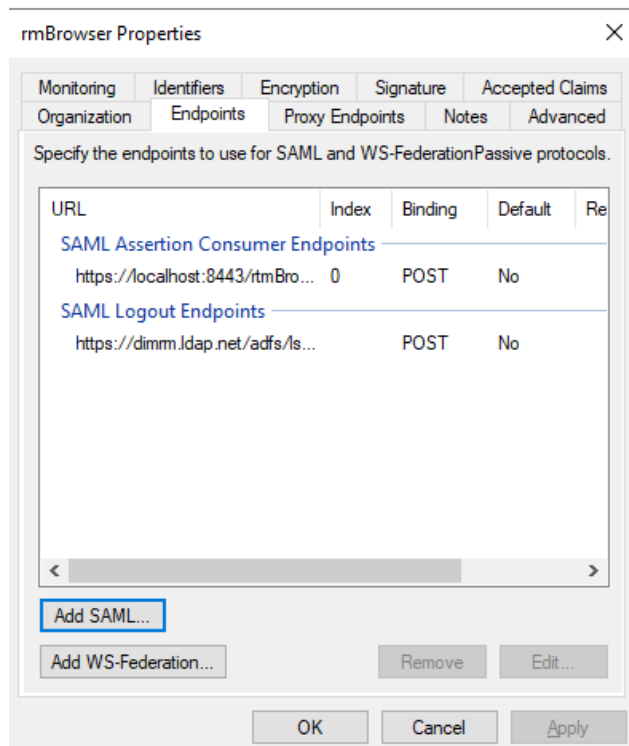
- 1 Open the AD FS Management application
- 2 In the tree select Relying Party Trusts folder.
- 3 In the Actions Pane select *Add Relying Party Trust*.



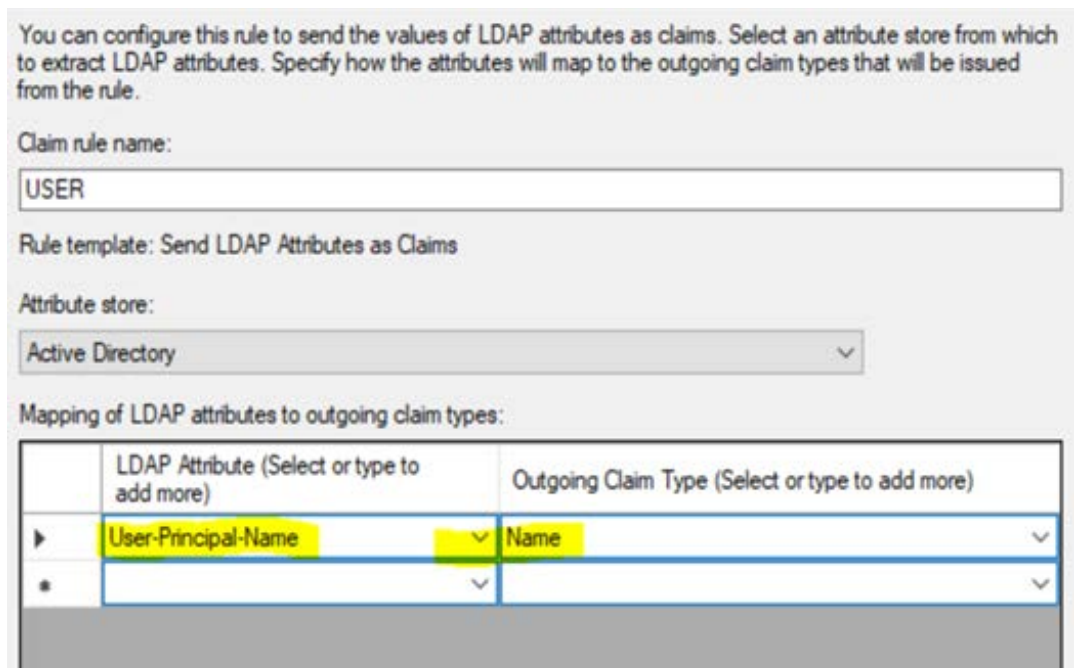
- 4 Click 'Start'
- 5 From 'Welcome to the Add Relying Party Trust' dialog:
  - a Select 'Claims Aware'
  - b Click 'Next'

- 6** From 'Select Data Source' dialog:
  - a** Select 'Enter data about the relying party manually'
  - b** Click 'Next'
- 7** From 'Specify Display Name' dialog:
  - a** Enter 'Display Name' e.g., **RM Browser app**
  - b** Click 'Next'
- 8** From 'Configure URL' dialog:
  - a** Check the box 'Enable support for the SAML 2.0 Web SSO protocol'
  - b** Provide Relying party SAML 2.0 SSO service URL, e.g.,  
<https://localhost:8443/rtmBrowser/auth?saml2>
  - c** Click 'Next'
- 9** From 'Configure Identifiers' dialog:
  - a** Provide Relying party trust identifiers, e.g.,  
<https://localhost:8443/rtmBrowser/>
  - b** Click 'Add'
  - c** Click 'Next'
- 10** Choose Access Control Policy (e.g., Permit everyone), Click 'Next'
- 11** From 'Finish', Click 'Close'
- 12** Right mouse click on create 'Relying Party Trust',
  - a** Select Properties
  - b** Switch to the Endpoints tab
  - c** Click **Add SAML** button (see "[Select the relevant Outgoing claim type](#)" on page 117)
  - d** Select Endpoint Type: SAML Logout
  - e** Provide Trusted URL (adfs endpoint + /?wa=wsignout1.0 )
- 13** On the Relying Party Trusts dialog:
  - a** Select your application
  - b** Select 'Edit Claim Issuance Policy' in the Actions Pane
  - c** Click 'Add Rule'
- 14** On the 'Select Rule Template' dialog:
  - a** Under 'Claim Rule Template' select 'Transform an Incoming Claim'
  - b** Click 'Next'
- 15** On the Configure Rule dialog (see "[Select the relevant Outgoing claim type](#)" on page 117):
  - a** Under 'Claim rule name'
  - b** Enter the display name for this rule

- c Select the relevant Incoming claim type
- d Select the relevant Outgoing claim type



**Figure 4-3. Add SAML Dialog**



**Figure 4-4. Sample Rule**

## Part 2: Complete the Configuration in Dimensions RM

- 1 Stop Services:
  - a **Dimensions RM Common Tomcat**
  - a **Dimensions RM Pool Manager**
- 2 Copy *RM\_Install*\Common Tools #.#.#.#\tomcat\#.#\webapps\rtmBrowser\WEB-INF\web.xml to a backup - just to be safe.
- 3 Open *RM\_Install*\Common Tools #.#.#.#\tomcat\#.#\webapps\rtmBrowser\WEB-INF\web.xml with a text editor, e.g. Notepad.
- 4 Search for **SAML2 SSO Filter**
- 5 Modify as follows:
  - a Uncomment the filter section.
  - b Set enabled param-value to **true**
  - c Set audience to <https://localhost:8443/rtmBrowser/>
  - d Set Login to <https://dimrm ldap.net/adfs/ls/>
  - e Set Logout to <https://dimrm ldap.net/adfs/ls/?wa=wsignout1.0>

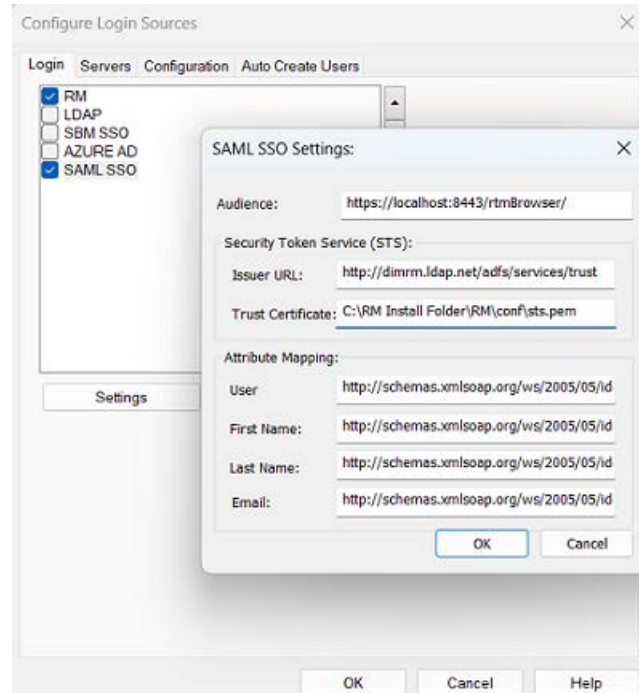


### NOTE

If the preference is that logout only logout from the Dimensions RM application, then the logout param value should be empty.

```
<param-name>logout</param-name>  
<param-value></param-value>
```

- f Save web.xml
- 6 Execute RM Manage as administrator
  - a Right click database name, choose Configure Login Sources
  - b Configure login sources, checking **RM** and **SAML SSO** (see "[Configure SAML SSO Login](#)" on page 119).
  - c Click the 'Settings' box
  - d Set Audience: <https://localhost:8443/rtmBrowser/>
  - e Set Issuer URL: <http://dimrm ldap.net/adfs/services/trust>
  - f Click OK



**Figure 4-5. Configure SAML SSO Login**

- 7 Select the 'Auto Create Users' tab on Configure Login Sources
  - a Enable Auto Create
  - b Enter the name of the instance into which users will be created
  - c Select the default Group and enable Assign to Categories
- 8 Export the Trust Certificate
  - a Export the certificate from the AD FS server in pem format
  - b Save it as sts.pem and copy it to RM\conf folder and name as sts.pem (see ["Configure SAML SSO Login" on page 119](#)).
- 9 **Terminate all running rmLicenseAgent.exe instances in Task Manager**
- 10 Re-start Services:
  - a **Dimensions RM Common Tomcat Service**
  - b **Dimensions RM Pool Manager**
- 11 Login to RM Browser. You should be redirected to AD FS SSO and validated successfully.

## 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\Micro Focus\Dimensions RM\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\Open Text\Dimensions 25.2\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\Open Text\Dimensions 25.2\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\Open Text\Dimensions 25.2\RM\conf\sts.pem

RM Server Registry Keys	
Key	Description
SSO_RELIVING_PARTY	<p>Should contain the SSO "Reliving Party" used to validate and request Token. For more information about this value, read the STS server configuration information</p> <p>Contains a default value of:</p> <pre>uri:org:eclipse:alf:sso:relyingparty :anonymous:anonymous:anonymous;uri :org:eclipse:alf:sso:relyingparty :serena.application.engine .notification.server:anonymous :anonymous</pre>
SSO_CLOCK_TOLERANCE	<p>"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.</p> <p>Value set by the installer: 300</p>

### Gatekeeper Parameters

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

```
<RM_Install_Dir>\Dimensions 25.2\Common Tools
  2.5.0.0\tomcat\10.1\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.

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

<b>gatekeeper-services-config.xml</b>	
<b>Parameter</b>	<b>Description</b>
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\Micro Focus\Dimensions RM\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\Open Text\Dimensions 25.2\RM\conf\r mkey.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\Open Text\Dimensions 25.2\RM\conf\r mcert.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.  <b>NOTE</b> 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 [Table , "Exporting a Certificate from the STS Server," on page 113.](#)

**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.

## Redirecting Internal Web Service and REST Service Calls

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

**To redirect internal web service calls, do the following:**

- 1 Open Windows Registry editor (select **Run**, enter `regedit` and click **OK**).
- 2 Navigate to  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Micro Focus\Dimensions RM\Environment\Default.
- 3 Right-click the **Default** key and select **New | String Value** from the shortcut menu.
- 4 Specify the name `RM_INTERNAL_WS_URL` and press **Enter**.
- 5 Double-click the `RM_INTERNAL_WS_URL` value. This opens the **Edit String** dialog.
- 6 Enter the server URL into the **Value data** box, e.g. `http://localhost:8080/`  
If HTTP is not enabled, change the URL protocol to `https`.  
Change the port to match your Tomcat configuration.
- 7 Click **OK**.

**To redirect internal REST service calls, do the following:**

- 1 Open Windows Registry editor (select **Run**, enter `regedit` and click **OK**).
- 2 Navigate to  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Micro Focus\Dimensions RM\Environment\Default.
- 3 Right-click the **Default** key and select **New | String Value** from the shortcut menu.
- 4 Specify the name `RM_INTERNAL_REST_URL` and press **Enter**.
- 5 Double-click the `RM_INTERNAL_REST_URL` value. This opens the **Edit String** dialog.
- 6 Enter the server URL into the **Value data** box, e.g. `http://localhost:8080/`  
If HTTP is not enabled, change the URL protocol to `https`.  
Change the port to match your Tomcat configuration.
- 7 Click **OK**.



# Test Management

# Test Management

We continue to progress with our migration from System Administration tasks that must be completed using RM Manage to Instance Administration Tasks completed in the Browser. As of the 12.12 (24.3) release, all functions associated with the class definition and implementation of Test Management can now be accomplished by the Instance Administrator.

The tasks associated with the implementation and application of Test Management are located in Chapter 9 of the *RM Browser User's Guide*.



## NOTE

Test Management functionality was expanded in Dimensions RM release 12.11.1, and continues to be expanded with each new release. If your organization installed and implemented Test Management prior to 12.11.1, please submit a support request together with the current release of Dimensions RM.

We do not recommend installing the new classes directly into an instance with pre-12.11.1 Test Management classes installed. If you have questions or concerns, please contact support.





# Chapter 6

---

## Logging

Log Files	132
Logging Administrative Activities	135

---

# Log Files

## Logging Configuration File log4cpp.conf

The logging configuration file (<RM Install Dir>\conf\log4cpp.conf by default) controls some of the behavior of the integration between Dimensions RM and another application:

- Level of detail (DEBUG, INFO, WARN, ERROR). For further information about log levels, see chapter ["Log Levels" on page 134](#).
- Location of the log file
- Name of the log file
- Maximum size of the log file. For further information about the log file size, see chapter ["Controlling Log File Size" on page 133](#).

The maximum number of log files that are maintained as a result of "rolling" to additional files after a log file reaches the maximum size limit

The log4cpp.conf file contains these categories:

- fileBrowser
- fileManage
- fileSyncEngine
- fileWebService
- fileAlfEventEmitter
- fileIcCheck
- PoolManager
- fileRTMLS
- fileClasDef
- fileXMLTooling
- fileMailService
- fileMailConfig

You can change the level of detail by replacing the default value (WARN) with one of the other values described in chapter ["Log Levels" on page 134](#).

You can change the location of the log file by updating the log4cpp.conf file. You can also change the name of the log file.

To control the size of the log file, see ["Controlling Log File Size,"](#) below.

The layout of the output of the log file is controlled by the log4j.appender.fileALFEventEmitter.layout settings, which use standard log4j formatting.



**CAUTION!** You should not change anything else in the log4cpp.conf file.

## Controlling Log File Size

There are two possible settings for `log4j.appender.fileALFEventEmitter<category>`, which controls how information gets appended to the log. The simplest configuration lets the log file grow indefinitely:

```
log4j.appender.fileALFEventEmitter=org.apache.log4j.FileAppender
```

However, it is more likely that you want to limit the maximum size of the log file so that it does not consume excessive system resources. To do this, specify a "rolling file appender", which starts a new file (such as `ALFEvents.log2`) after the first file exceeds the specified size limit. In the following example, the maximum file size is 5,000,000 bytes, and no more than three (the most recent three) log files are retained.

```
log4j.appender.fileALFEventEmitter=org.apache.log4j.
    RollingFileAppender
log4j.appender.fileALFEventEmitter.maxFileSize=5000000
log4j.appender.fileALFEventEmitter.maxBackupIndex=3
```

Note that if you set `log4j.appender.fileALFEventEmitter.append` to `false` and you are using the rolling file appender, the emitter service starts a new log file each time that you start the service, regardless of whether the maximum file size was reached.

If you are not using the rolling file appender and you set `log4j.appender.fileALFEventEmitter.append` to `false`, the emitter service overwrites the log file each time the service starts.

## Logging Configuration File `log4net.config`

The logging configuration file (`<RM Install Dir>\conf\log4net.config` by default) controls the behavior of how the log file is written:

- Level of detail (DEBUG, INFO, WARN, ERROR). For further information about log levels, see chapter "[Log Levels](#)" on page 134.
- Location of the log file
- Name of the log file
- Maximum size of the log file. For further information about the log file size, see chapter "[Controlling Log File Size](#)" on page 134.

The maximum number of log files that are maintained as a result of "rolling" to additional files after a log file reaches the maximum size limit

The `log4net.config` file contains configurations for these applications/functionalities:

- `RMImport`
- `WordDocumentPostProcessor`
- `DashboardExport`
- `ExcelFormatConverter`
- `ForceExit`
- `WordPublishSupport`
- `ServiceHelper`

You can change the level of detail by replacing the default value (INFO) with one of the other values described in chapter "[Log Levels](#)" on page 134.

You can change the location of the log file by updating the `log4cpp.conf` file. You can also change the name of the log file.

To control the size of the log file, see "[Controlling Log File Size](#)," below.

The layout of the output of the log file is controlled by the `log4net.Layout.PatternLayout` settings, which use standard log4net formatting.



**CAUTION!** You should not change anything else in the `log4net.config` file.

### Controlling Log File Size

The `log4net.config` file allows to limit the maximum size of the log file so that it does not consume excessive system resources. To do this, specify a "rolling file appender", which starts a new file (such as `RMImport.log.2`) after the first file exceeds the specified size limit. In the following example, the maximum file size is 1,048,576,000 bytes, and no more than ten (the most recent ten) log files are retained.

```
<param name="MaximumFileSize" value="1000KB"/>
<param name="MaxSizeRollBackups" value="10"/>
```

Note that if you set `AppendToFile` to `false` and you are using the rolling file appender, the application (e.g. RM Import) or functionality used by Dimensions RM server (e.g. Word Publish Support) starts a new log file each time it is executed, regardless of whether the maximum file size was reached. You might set this for RM Import as it is a client application, for all other configurations, this is not recommended.

## Log Levels

A log file can contain different levels of information. The following table shows the different log level configuration and the resulting information in the log file. The log levels described below are valid for both configuration files, `log4cpp.conf` and

Log Level	Description	Log Levels included in Log File
ERROR	Shows operations that failed. Error is the most restrictive level of logging.	<ul style="list-style-type: none"> <li>■ ERROR</li> </ul>
WARN	Provides notification that an operation completed, but there were potential problems with the operation, e.g. output problems with the database or XML file configuration, undefined fields, or value truncation.	<ul style="list-style-type: none"> <li>■ ERROR</li> <li>■ WARN</li> </ul>

Log Level	Description	Log Levels included in Log File
INFO	Provides general information about an operation.	<ul style="list-style-type: none"> <li>■ ERROR</li> <li>■ WARN</li> <li>■ INFO</li> </ul>
DEBUG	Provides step-by-step information about an operation. Debug is the highest level of logging.	<ul style="list-style-type: none"> <li>■ ERROR</li> <li>■ WARN</li> <li>■ INFO</li> <li>■ DEBUG</li> </ul>

## Logging with RM Import

### To create a log file for RM Import:

- 1 Open the file <RM Install Dir>\conf\log4net.conf with a text editor, e.g. Notepad.
- 2 To change the log level, do the following:
  - a Find the <level tag which precedes the <appender-ref ref="RMImportFile" /> tag.
  - b Change the value attribute to your desired log level. The default is INFO. The whole level tag may look like this: <level value="INFO" />  
For further information about log levels, see chapter ["Log Levels" on page 134](#).
- 3 To change the maximum file size, do the following:
  - a Find the <param name="MaximumFileSize" tag.
  - b Set the value attribute to your desired file size. The default is 1000KB. You may also specify the file size in MB, e.g. 8MB.
- 4 Start RM Import or RM Import Designer. An RMImport.log file is generated in the <RM Install Dir>\logs directory, and reports errors that are generated, if any.

## Logging Administrative Activities

### About Administrative Logging

Dimensions RM logs administrative activity by recording relevant data, such as the user ID of the administrative user and the change that they made. This information is stored in the RM database in a table named ADM\_USERS\_ACTIVITY. When accessing the database directly (Oracle: SQL\*Plus, MS SQL Server: SQL Server Management Studio), administrative users can invoke three types of operations upon this data:

- **Archive** operations move data of a certain age from the ADM\_USERS\_ACTIVITY table to the ADM\_USERS\_ACTIVITY\_HISTORY table. This allows you to reduce the size of the active table while still retaining the data for future reference. See ["Archive Operations under Oracle" on page 140](#).

- **Remove** operations delete data of a certain age from both tables. See ["Remove Operations" on page 141](#).
- **Show** operations display, or export to a file, data that meets specified arguments, such as activity that occurred during a specific date range or that was performed by a specific user. See ["Show Operations" on page 142](#).

In all cases, the administrative user must first connect to the database (Oracle via SQL\*Plus; MS SQL Server via SQL Server Management Studio). See the following sections for details specific to each type of operation.



**NOTE** See ["Actions for which Data Is Recorded" on page 136](#) for a list of the data that is recorded for each administrative action.

## Actions for which Data Is Recorded

The following table lists the data that is recorded specific to each administrative action. The strings shown in the **Action** column are the values that can be used for the ARG\_ACTION argument of a Show operation.



**NOTE** In all cases, the user ID that initiated the action and the date and time are recorded.

Information Recorded by Activity	
Action	Data Recorded
ADD_GROUP_TO_PROJECT	Group name Instance name
ADD_USER_TO_GROUP	User name Group name
ADD_USER_TO_PROJECT	User name Instance name
ADMINISTER_EMAIL	Instance name Class name
ASSOCIATE_TO_DIM_CM	Association information
BACKUP_PROJECT	Instance name
BACKUP_PROJECT_SCHEMA	Schema name
CATEGORY_CREATED	Category name
CATEGORY_DELETED	Category Name
CATEGORY_MODIFIED	Category name
CHANGE_PASSWORD_RULES	Settings that were changed Modified values before and after
CHANGE_PROJECT_PASSWORD	User name (if InstanceAdmin PW) Instance name (if Oracle PW)
CHANGE_USER_PASSWORD	User name

Information Recorded by Activity	
Action	Data Recorded
CLASS_ATTRIBUTES_CHANGED	Instance name Class name Attribute name Modified values before and after
CLASS_CREATED	Instance name Class name
CLASS_DELETED	Instance name Class name
CLASS_MODIFIED	Instance name Class name Modified values before and after
CLASS_TYPE_CREATED	Instance name Class type name
CLASS_TYPE_DELETED	Instance name Class type name
CLASS_TYPE_MODIFIED	Instance name Class type name Modified values before and after
CLASS_TYPE_ATTRIBUTES_CHANGED	Instance name Class type name Attribute name Modified values before and after
CONFIGURE_ALF_OPTIONS	Instance name Modified values before and after
CONFIGURE_LOGIN_SOURCES	Instance name Modified values before and after
CREATE_GROUP	Group name
CREATE_PROJECT	Instance name
CREATE_USER	User name
DELETE_GROUP	Group name
DELETE_PROJECT	Instance name
DELETE_USER	User name
DISABLE_PERMISSIONS_INHERITANCE_FROM_PARENT_CATEGORY	Category name Instance name
DROP_PROJECT_TABLES	Instance name
ENABLE_PERMISSIONS_INHERITANCE_FROM_PARENT_CATEGORY	Category name Instance name
GRANT_ACCESS_RIGHT_TO_USER	Instance name User name Access right granted
GRANT_ACCESS_RIGHT_TO_GROUP	Instance name Group name Access right granted

Information Recorded by Activity	
Action	Data Recorded
GRANT_CATEGORY_TO_GROUP	Instance name Group name Category name
INSTALL_PROJECT_TABLES	Instance name
LOGIN_ATTEMPT_TO_DATABASE	User name Database name Client name Failure reason
LOGIN_ATTEMPT_TO_PROJECT	User name Instance name Client name Failure reason
LOGIN_USER_TO_DATABASE	User name IP address Database name Client name
LOGIN_USER_TO_PROJECT	User name IP address Instance name Client name
LOGOUT_FROM_DATABASE	User name
LOGOUT_FROM_PROJECT	Instance name User name
MODIFY_GROUP	Group name Modified values before and after
MODIFY_USER	User name Modified values before and after
PLACE_PROJECT_OFFLINE	Instance name
PLACE_PROJECT_ONLINE	Instance name
PROPERTIES_PROJECT	Instance name Modified values before and after
RECREATE_DATABASE_INDEXES	Instance name
RECREATE_DATABASE_PROCEDURES	Instance name
RECREATE_DATABASE_RESOURCES	Instance name
RELATIONSHIP_ATTRIBUTES_CHANGED	Instance name Relationship name Attribute name Modified values before and after
RELATIONSHIP_CONSTRAINTS_CHANGED	Instance name Relationship name Constraint name Modified values before and after
RELATIONSHIP_CREATED	Instance name Relationship name

Information Recorded by Activity	
Action	Data Recorded
RELATIONSHIP_DELETED	Instance name Relationship name
RELATIONSHIP_MODIFIED	Instance name Relationship name Modified values before and after
REVOKE_CATEGORY_FROM_USER_IN_GROUP	Category name Group name Instance name
REMOVE_GROUP_FROM_PROJECT	Instance name Group name
REMOVE_USER_FROM_GROUP	Group name User name
REMOVE_USER_FROM_PROJECT	Instance name User name
RESTORE_PROJECT	Instance name
RESTORE_PROJECT_SCHEMA	Schema name
REVOKE_ACCESS_RIGHT_FROM_GROUP	Instance name Group name Access right
REVOKE_ACCESS_RIGHT_FROM_USER	Instance name User name Access right
REVOKE_CATEGORY_FROM_GROUP	Instance name Group name Category name
REVOKE_CATEGORY_FROM_USER_IN_GROUP	Instance name Category name Group name User Name
REVOKE_EXPLICITLY_ACCESS_RIGHT_FROM_GROUP	Instance name Group name Access right
REVOKE_EXPLICITLY_ACCESS_RIGHT_FROM_USER	Instance name User name Access right
REVOKE_EXPLICITLY_CATEGORY_FROM_GROUP	Instance name Group name Category name
WORKFLOW_DISABLED	Instance name Class name
WORKFLOW_ENABLED	Instance name Class name
WORKFLOW_STATE_CREATED	Instance name Class name State name

Information Recorded by Activity	
Action	Data Recorded
WORKFLOW_STATE_DELETED	Instance name Class name State name
WORKFLOW_STATE_MODIFIED	Instance name Class name State name Description of modification
WORKFLOW_STATE_RENAMED	Instance name Class name State name New state name
WORKFLOW_TRANSITION_CREATED	Instance name Class name Transition name
WORKFLOW_TRANSITION_DELETED	Instance name Class name Transition name
WORKFLOW_TRANSITION_MODIFIED	Instance name Class name Transition name Description of modification
WORKFLOW_TRANSITION_RENAMED	Instance name Class name Transition name New transition name

## Archive Operations under Oracle

Archive operations move data of a certain age from the ADM\_USERS\_ACTIVITY table to the ADM\_USERS\_ACTIVITY\_HISTORY table. This allows you to reduce the size of the active table while still retaining the data for future reference.

### Syntax

```
"exec ICADMIN.PKG_AUDIT.ARCHIVE_USERS_ACTIVITY
  (' ARG_FROM_DATE' , ' ARG_TO_DATE' , ' ARG_DATE_FORMAT' );"
```

This command can be run via SQL\*Plus on either the server or a client system.

### Arguments

Archive operations have three optional arguments. The arguments are position dependent, so you must specify them in the correct order and include a null value for any argument that is being skipped over on the way to a later argument in the sequence.

#### ARG\_FROM\_DATE

Specifies the date, or date and time, of the oldest records to be moved. The default is 01-JAN-1900.

### **ARG\_TO\_DATE**

Specifies the date, or date and time, of the newest records to be moved. The default is the current date minus three months.

### **ARG\_DATE\_FORMAT**

Specifies the date and time format used by the ARG\_FROM\_DATE and ARG\_TO\_DATE arguments. By default, the format defined by the NLS\_TIMESTAMP\_FORMAT parameter of the current session is used.

## **Examples**

### **Example 1: Default**

```
"exec ICADMIN.PKG_AUDIT.ARCHIVE_USERS_ACTIVITY( );"
```

**Result:** All records between January 1, 1900 and the current date minus three months are moved to the History table.

### **Example 2: Specific Date Range**

```
"exec ICADMIN.PKG_AUDIT.ARCHIVE_USERS_ACTIVITY('15-JAN-2011', '30-MAY-2011');"
```

**Result:** All records between January 15, 2011 and May 30, 2011 are moved to the History table.

### **Example 3: Specific Starting Date and Date Format**

```
"exec ICADMIN.PKG_AUDIT.ARCHIVE_USERS_ACTIVITY('15/01/2011', null, 'dd/mm/yyyy');"
```

**Result:** All records between January 15, 2011 and the current date minus three months are moved to the History table. For this operation, the value of the NLS\_TIMESTAMP\_FORMAT parameter is overridden allowing the use of the dd/mm/yyyy format.

## **Remove Operations**

Remove operations delete data of a certain age from the ADM\_USERS\_ACTIVITY and ADM\_USERS\_ACTIVITY\_HISTORY tables. Both tables are acted upon; you cannot act on just one of the tables.

### **Syntax**

```
"exec ICADMIN.PKG_AUDIT.REMOVE_USERS_ACTIVITY
  (' ARG_FROM_DATE', ' ARG_DATE_FORMAT' );"
```

This command can be run via SQL\*Plus on either the server or a client system.

### **Arguments**

Remove operations have two optional arguments. The arguments are position dependent, so you must specify them in the correct order.

**ARG\_FROM\_DATE**

Specifies the date, or date and time, of the newest records to be deleted. All records equal to or older than the specified date will be deleted. The default is to delete all records older than 12 months.

**ARG\_DATE\_FORMAT**

Specifies the date and time format used by the ARG\_FROM\_DATE argument. By default, the format defined by the NLS\_TIMESTAMP\_FORMAT parameter of the current session is used.

**Examples****Example 1: Default**

```
"exec ICADMIN.PKG_AUDIT.REMOVE_USERS_ACTIVITY();"
```

**Result:** All records older than 12 months are deleted.

**Example 2: Specific Starting Date**

```
"exec ICADMIN.PKG_AUDIT.REMOVE_USERS_ACTIVITY('30-MAY-2011');"
```

**Result:** All records equal to or older than May 30, 2011 are deleted.

**Show Operations**

Show operations display, or export to a file, data that matches specified arguments, such as activity that occurred during a specific date range or that was performed by a specific user.

**Syntax**

The data can be output to the system screen or exported to a CSV file. The syntax to export to a CSV differs from the screen output syntax and must be run on a client system.

**Screen Dump Syntax**

```
"set serveroutput on size 1000000;"  
"exec ICADMIN.PKG_AUDIT.SHOW_USERS_ACTIVITY  
  ('ARG_USER', 'ARG_ACTION', 'ARG_FROM_DATE', 'ARG_TO_DATE',  
  'ARG_DATE_FORMAT', 'ARG_USE_ARCHIVE');"
```

This command can be run via SQL\*Plus on either the server or a client system.

**Export to CSV File Syntax**

```
spool "OutPutPath\FileName.csv"  
set heading off  
set serveroutput on size 1000000  
exec ICADMIN.SHOW_USERS_ACTIVITY  
  ('ARG_USER', 'ARG_ACTION', 'ARG_FROM_DATE', 'ARG_TO_DATE',  
  'ARG_DATE_FORMAT', 'ARG_USE_ARCHIVE');  
spool off
```

This command is to be run on a client system via SQL\*Plus. The results are exported to a CSV file on the client system.

## Arguments

Show operations have six optional arguments. The arguments are position dependent, so you must specify them in the correct order and include a null value for any argument that is being skipped over on the way to a later argument in the sequence.

### ARG\_USER

Specifies a user name. If a name is specified, only records of that user's actions will be displayed. Else, the records of all users will be displayed.

### ARG\_ACTION

Specifies a specific user action. If an action is specified, only records of that type of action will be displayed. Else, records of all action types will be displayed. See ["Actions for which Data Is Recorded" on page 136](#) for a list of the actions that can be specified.

### ARG\_FROM\_DATE

Specifies the date, or date and time, of the oldest records to be displayed. The default is 01-JAN-1900.

### ARG\_TO\_DATE

Specifies the date, or date and time, of the newest records to be displayed. The default is 01-JAN-2049.

### ARG\_DATE\_FORMAT

Specifies the date and time format used by the ARG\_FROM\_DATE and ARG\_TO\_DATE arguments. By default, the format defined by the NLS\_TIMESTAMP\_FORMAT parameter of the current session is used.

### ARG\_USE\_ARCHIVE

Specifies whether records are displayed from just the ADM\_USERS\_ACTIVITY table (the default) or from both it and the ADM\_USERS\_ACTIVITY\_HISTORY table. To include records from the History table, use **1** as the value for this argument.

## Examples

### Example 1: Default - Output to File

```
spool "C:\RM_audit.csv"  
set heading off  
set serveroutput on size 1000000  
exec ICADMIN.SHOW_USERS_ACTIVITY();  
spool off
```

**Results:** Creates a file named RM\_audit.csv on the client system. It contains all records in the ADM\_USERS\_ACTIVITY table of events that occurred between January 1, 1900 and January 1, 2049. Records that have been moved to the ADM\_USERS\_ACTIVITY\_HISTORY table are not included.

### Example 2: Specific User and Date Range - Output to Screen

```
"set serveroutput on size 1000000;"
"exec ICADMIN.PKG_AUDIT.SHOW_USERS_ACTIVITY
  ('bsmith',null,'01-JAN-2011','30-MAY-2011');"
```

**Results:** Outputs to the screen the records of all actions taken by the user **bsmith** between January 1, 2011 and May 30, 2011. Records that have been moved to the ADM\_USERS\_ACTIVITY\_HISTORY table are not included.

### **Example 3: Specific Action and Include History - Output to File**

```
spool "C:\RM_audit_AddUsers.csv"
set heading off
set serveroutput on size 1000000
exec ICADMIN.SHOW_USERS_ACTIVITY(null,'ADD_USER_TO_PROJECT',null,
  null,null,'1');
spool off
```

**Results:** Creates a file named RM\_audit\_AddUsers.csv on the client system. It contains all records where a user was added to an instance between January 1, 1900 and January 1, 2049. The results include records in the ADM\_USERS\_ACTIVITY table as well as those that have been moved to the ADM\_USERS\_ACTIVITY\_HISTORY table.

## Chapter 7

---

# Application Lifecycle Framework (ALF)

Overview	146
Architecture	146
Emitting ALF Events	147
Dimensions RM Web Services	149
Enabling an Instance for ALF	150
Configuring the ALF Emitter Service	151
Using SSL Authentication with ALF	153
Logging	155
Troubleshooting	155

## Overview

This chapter describes how to emit Application Lifecycle Framework (ALF) events from Dimensions RM and the Web services needed to implement an integration between Dimensions RM and another application, for example, Dimensions CM.

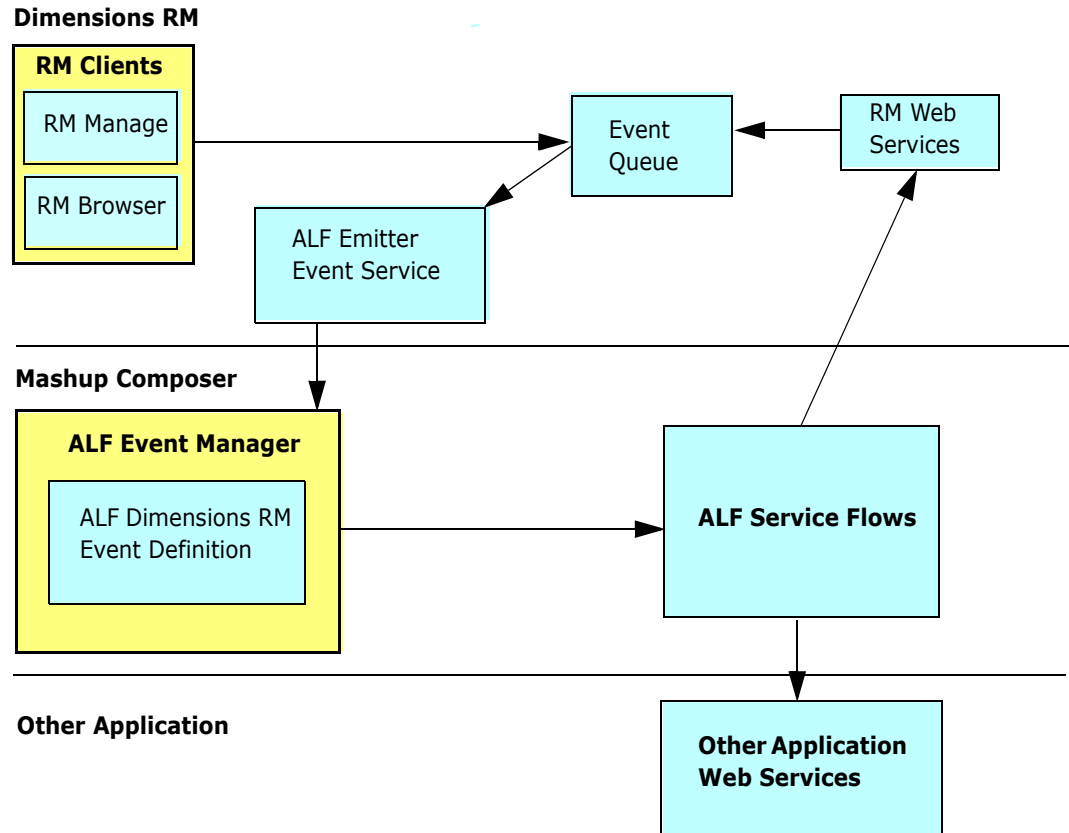
The following prerequisites must be met before you can implement integration:

- Solution Business Manager (SBM) Composer—An Open Text visual interface for creating and designing mashups, which are Web applications that mix information from more than one source into a single application. Solution Business Manager Composer lets you manipulate applications and orchestration workflows to meet specific business needs.
- Web services—You must understand Web services and how they interoperate in custom ways.
- ALF—You must have a working knowledge of ALF. ALF defines an open source framework which, when adhered to, enables applications to interact using Web services, events, and BPEL process. Download the archived ALF project home page on [www.eclipse.org/alf](http://www.eclipse.org/alf) for more information.

## Architecture

To be involved in an ALF-based integration, Dimensions RM must emit ALF events and send notifications to the ALF Event Manager, which starts ALF service flows that are defined in Mashup Composer. The service flows contain the rule that decides when and how to create items in each application.

The following flowchart illustrates the integration architecture.



**Figure 7-1. Integration Architecture**

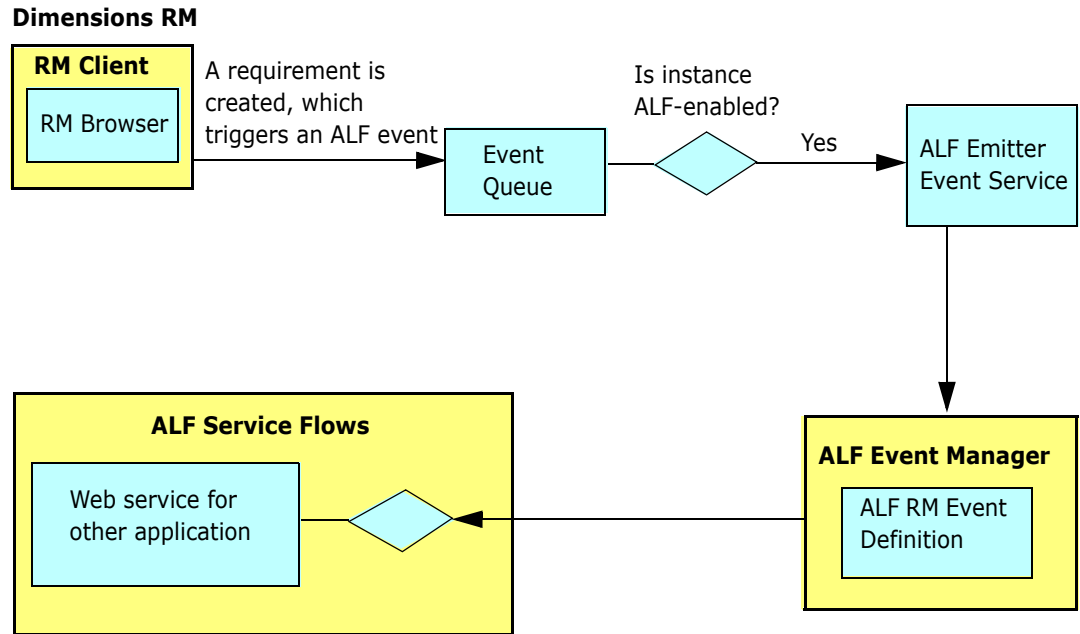
## Emitting ALF Events

An *event* is a Web service message sent from Dimensions RM to the ALF infrastructure. The Event Manager defines an event Web service as the interface for ALF events, and Dimensions RM calls this Web service to emit events.



**NOTE** Before emitting an event, Dimensions RM determines whether the Dimensions RM instance is an ALF-enabled instance. The check box on the **Configure ALF Options** dialog box determines this. For more information about making an instance an ALF-enabled instance, see ["Enabling an Instance for ALF" on page 150](#).

The following flowchart illustrates the process of emitting an event from Dimensions RM.



**Figure 7-2. Emitting an Event from Dimensions RM**



**NOTE** The decision block in the **ALF Service Flows** segment of the flowchart depends on the service flow design. For example, suppose you want to create an item in another application when a Dimensions RM requirement is moved to a collection named "Scoping." The decision block would determine whether the event type is "Add to Collection" and accordingly it should create the item in the other application.

Dimensions RM emits events on predefined trigger points, which are defined in the following section. Any condition check for the integration data synchronization is handled in the service flow.

## Trigger Points

The following table describes the trigger points that cause Dimensions RM to emit ALF events.

Trigger Point	Object Type	Event Type
Requirement is created	Requirement	create
Requirement is updated or replaced	Requirement	update
Requirement is deleted or removed	Requirement	delete
Requirement is moved to a collection	Requirement	addToCollection
Requirement is removed from a collection	Requirement	removeFromCollection
Attachment is added to a requirement	Requirement	attachmentAdded
Attachment is removed from a requirement	Requirement	attachmentRemoved
Attachment is updated	Requirement	attachmentUpdated

Trigger Point	Object Type	Event Type
Requirement is linked	Link	create
Requirement is unlinked	Link	delete

## Event Definition

The ALF event definition consists of the following:

- ALF Object Type—A string (for example, *Requirement*).
- ALF Event Type—A string (for example, *create*, *delete*, and so on).
- Custom extension data structure for a requirement or link. The custom extension data structure consists of database name, instance name, requirement type, object ID, PUID, and user name. For the "addToCollection" and "removeFromCollection" events, the collection name is included in the extension data. For link events, the target requirement information is added to the extension data.

If there is a failure in the invocation of the event, error messages will be logged in the log file. For information about logging, see ["Logging" on page 155](#).

## Event Emitter

A standalone Microsoft® Windows service emits queued ALF events according to the interval specified in the ALFEventConfig.xml file. Events (for example, creating requirements) are not sent in real time, but according to these intervals.

The ALFEventConfig.xml file is stored in the <RM Install Dir>\conf directory.

## Event Emitter Service

For information about starting and running the event emitter service, see ["Configuring the ALF Emitter Service" on page 151](#).

# Dimensions RM Web Services

Dimensions RM provides CRUD (create, read, update, delete) Web services that can be used for ALF service flows.

The following methods have been added to the existing Web services to support ALF.

Method	Description
AddSyncXrefLink	Creates a reference entry in the SYNC_XREF table, which can be used to store association information between Dimensions RM and the other tool.
CreateObject	Creates a requirement in the specified class.
DeleteAttachment	Deletes the specified requirement attachment.

Method	Description
DeleteObjects	Deletes the requirement. This is a soft delete, which deletes the requirement from the instance but not from the database.
DeleteSyncXrefLink	Removes the reference entry between Dimensions RM and the other tool.
GetObjectsInCollection	Gets objects in specific collections.
LinkObjects	Creates a link between two requirements.
ListCollections	Gets a list of collections in the instance.
ListObjectLinks	Lists all of the links for a requirement.
ReadObject	Returns information about a requirement.
ReadObjectAttachment	Returns information about requirement attachments.
ReadObjects	Returns information about requirements by reading multiple requirement identities (ids) at once. This is similar to ReadObject, but improves performance as multiple Requirements can be read by their ids in one call.  Parameters: -sessionid      The current session identifier.  -requirements    A list combination of PUID/ Classname or objectID/ Classname that specifies instance requirements.
ReadSyncXRefLink	Gets the reference item information.
UnLinkObjects	Removes the link between two requirements.
UpdateObject	Updates a requirement.
UpdateObjectAttachment	Updates requirement attachments.

For the full syntax and the parameters for these methods, see the Web services HTML reference information downloadable as a zip file from the Open Text Support Web site.

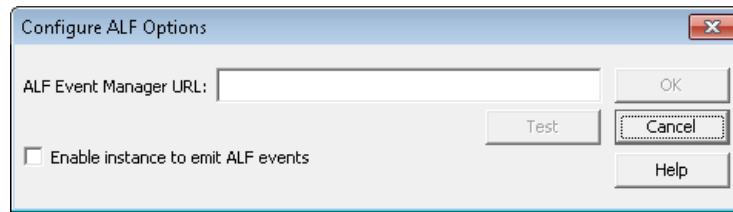
## Enabling an Instance for ALF

If an instance is an ALF-enabled instance, ALF events are emitted. Otherwise, ALF events are not emitted.

### To enable an instance to emit ALF events:

- 1 Start RM Manage.
- 2 Expand the database and select an instance.

- 3 Select **File | Configure ALF Options**. The **Configure ALF Options** dialog box opens.



**Figure 7-3. Configure ALF Options**

- 4 In the **ALF Event Manager URL** field, type the URL of the Event Manager server.
- 5 Click **Test** to validate the Event Manager URL. If the test fails, a message is displayed.
- 6 Select the **Enable instance to emit ALF events** check box if you want to make the instance an ALF-enabled instance.



**NOTE** The ALF Event Manager URL follows this format:

`http://servername:port/eventmanager/services/ALFEventManager`

**Example:** `http://myserver:8085/eventmanager/services/ALFEventManager`

## Configuring the ALF Emitter Service

The following sections describe how to configure the ALF emitter service.

### Usage

The command-line usage for the emitter service is as follows:

```
ALFEventEmitter [-f file] [-c] [-e level] [-E file] [-L priority]
  [-k {install|config|uninstall|start|stop}] [-n service_name] [-v]
  [-h] [-p password] [-l identifier] [-P eventName]
```

## Options

The options shown in [Usage](#) are described in the following table.

Option	Description
-c	Validates the <code>AlfEventConfig.xml</code> file against the associated schema document. The schema document is specified at the top of the <code>AlfEventConfig.xml</code> file. By default, this file is <code>ALFEventEmitter.xsd</code> and is located in the <code>&lt;RM Install Dir&gt;\conf</code> directory. After validating the document and logging any errors, the emitter service quits without any further processing.
-e <i>level</i>	Shows startup errors of the following levels: debug, info, warn, error.
-E <i>file</i>	Logs startup errors to a file.
-f <i>file</i>	Specifies an alternative configuration file.
-h	Lists the available command-line options.
-k <i>install</i>	Installs an <code>AlfEventEmitter</code> service.
-k <i>config</i>	Changes the startup options of an <code>AlfEmitter</code> service.
-k <i>uninstall</i>	Uninstalls the emitter service.
-k <i>start</i>	Starts the emitter service.
-k <i>stop</i>	Stops the emitter service.
-l <i>identifier</i>	Specifies a value used for encrypting the password (used in combination with -p).
-L <i>priority</i>	Sets the Windows system priority for the emitter service. <code>servicePriority</code> must be <code>LOW</code> , <code>BELOWNORMAL</code> , <code>NORMAL</code> , <code>ABOVENORMAL</code> , <code>HIGH</code> , or <code>REALTIME</code> . If you do not specify this option, the emitter service runs under the default priority of <code>BELOWNORMAL</code> .
-n <i>name</i>	Sets the service name.
-p <i>password</i>	Encrypts the password text for use in the config file.
-v	Displays the version number.

## Using Encrypted Passwords

For security purposes, it is suggested to use an encrypted password in the `AlfEventConfig.xml` file.

**To use an encrypted password in the `AlfEventConfig` file, do the following:**

- 1 Open the `RM_Install\conf\AlfEventConfig.xml` file in a text editor, e.g. Notepad.

- 2 Locate the **SBMSSOAuth** tag.
- 3 Identify the user name (the value from the **user** attribute).
- 4 Open a command prompt.
- 5 Navigate to the *RM\_Install\bin* directory.
- 6 Type `AlfEventEmitter -p <your_password> -l <identifier>` and press **Enter**, e.g. `AlfEventEmitter -p rtm -l opentext`. This outputs the encrypted password. For the example, the output would be: Encrypted value="34C844CC40A557D1"
- 7 Copy the encrypted password (without the quotes) to the Windows clipboard.
- 8 Change back to the text editor with the `AlfEventConfig.xml` file.
- 9 For the **SBMSSOAuth** tag, ensure that both, **identifier** and decrypt **attribute** are present. If these attributes are not present, create them as empty attributes, e.g. `<SBMSSOAuth user="joe" password="" decrypt="" />`
- 10 **user:** Ensure that the correct user account is used.
- 11 **password:** Replace the current password with the encrypted password from the clipboard.
- 12 **identifier:** Replace the current identifier with the one you used in the `AlfEventEmitter` command line (the value following the `-l` option).
- 13 **decrypt:** Ensure that the value is **true**.  
Example for the values used in step 6:  
`<SBMSSOAuth user="joe" password="34C844CC40A557D1" decrypt="true" />`
- 14 Save the file.
- 15 Restart the **Dimensions RM ALF Event Emitter** service.

## Installation

To install the emitter service, use the `-k install` option. This creates an instance of the service with all the other parameters you specify.

To uninstall the emitter service, use the `-k uninstall` option. You must specify the same service name (`-n name`) that you used when you installed the service; otherwise, the service will not be uninstalled correctly.

## Using SSL Authentication with ALF

If you have configured secure sockets layer (SSL) as your authentication method for Open Text Solution Business Manager (SBM) and you are using ALF to integrate with SBM (formerly called Serena Business Mashups), you must complete the steps in this section. These steps are required in order to use Dimensions RM and ALF with SBM with SSL security enabled.

### To use SSL authentication with ALF:

- 1 Open the following file in a text or XML editor:

RM\_HOME\conf\ALFEventConfig.xml

- 2 Make sure that section such as the following is present and set correctly:

```
<SslAuthentications>  
<SslAuthentication authenticationtype="SOAP_SSL_DEFAULT"  
  cafilename="server.cer"  
  cafilepath=""  
  keyfile="client.pem"  
  keyfilepassword="password" />  
</SslAuthentications>
```

- 3 Set the attributes as follows:

- **authenticationtype**

Set to any of the following:

- SOAP\_SSL\_DEFAULT - Default Authentication mode
- SOAP\_SSL\_NO\_AUTHENTICATION - Disable server authentication
- SOAP\_SSL\_REQUIRE\_SERVER\_AUTHENTICATION - If the client requires the server to authenticate
- SOAP\_SSL\_REQUIRE\_CLIENT\_AUTHENTICATION - If the server requires the client to authenticate
- SOAP\_SSL\_SKIP\_HOST\_CHECK - If the client does not check the common name of the host in certificate
- SOAP\_SSL\_RSA - Use RSA
- SOAP\_SSLv3\_TLSv1 - Use SSL v3 and TLS v1 support by default
- SOAP\_TLSv1 - Use TLS v1 only

To have more than one authentication type, use a pipe to separate the types (|).  
For example: SOAP\_SSL\_DEFAULT | SOAP\_SSL\_SKIP\_HOST\_CHECK

If "authenticationtype" is blank then the emitter service will interpret the setting as SOAP\_SSL\_NO\_AUTHENTICATION

For details on authentication types, refer to the gSOAP guide:

<http://www.cs.fsu.edu/~engelen/soapdoc2.html>

- **cafilename**

Trusted certificate file name (this is needed to verify the server).

- **cafilepath**

Path to the directory with the trusted certificates.

- **keyfile**

Required only when the client must authenticate to the server.

- **keyfilepassword**

Password to read the key file.

- 4 Save the file.

---

## Logging

The emitter service provides log files that contain information about its current state. Furthermore, the `AlfEventConfig.xml` file can return to the emitter service information that needs to be written to the log file.



**NOTE** The file named `ALFEvents.log` contains startup information. The startup information describes what happens during the parsing of the `AlfEventConfig.xml` file and other activities by the emitter service before starting an event cycle.

This file contains information about the event cycles themselves. This is the file that you will check the most often.

## Troubleshooting

### ALF Event Emitter Service Fails on Startup

If the **ALF Event Emitter** service fails when starting it, this may be due to an incorrect password in the `AlfEventConfig.xml` file. For further information on encrypted passwords, see chapter "[Using Encrypted Passwords](#)" on page 152.



# Chapter 8

---

## RM Manage

RM Manage Overview	158
Configuring Workspace Options	158
Functions Available from RM Manage	161
Creating the ICDBA Account	161
Managing Instances	164
Managing Users and Groups	206
Managing Security	223
Managing Databases	235
Configuring E-Mail Notification	240
Login Sources	246
Setting Up Password Security	258
ALM Integration Between Dimensions CM and Dimensions RM	261
Command Line Parameters	261
Using RM Manage within the Amazon Cloud	262
RM Manage Toolbars	263

## RM Manage Overview

RM Manage is the Dimensions RM tool used by **System Administrators** to maintain the health of the Dimensions RM implementation.

There are two groups available for the assignment of actions associated with administration: **System Administrator** and **Administrator** (also referred to as **Instance Administrator**).

**System Administrator** - A group found only in RM Manage, includes those individuals granted the ability to execute System Administrator functions in RM Manage as well as to manage the Dimensions RM Environment.

- Instance creation, modification from RM Manage, and deletion,
- User and Group management across all Instances.



**IMPORTANT!** Only **System Administrators** have access to **Dimensions RM Manage**

**Administrator** (Instance Administrator) – Users with this role may perform all administration functions within the boundary of the assigned instance. For example, from RM Browser, the Administrator may:

- create users and groups or add existing users to their instance
- modify the instance schema definition, attribute settings, category definition
- set default instance settings

## Configuring Workspace Options

In this section we discuss setting or modifying RM Manage workspace options. Settings stored in the Registry require that RM Manage be **Run as Administrator**.

### Mandatory Tab:

- The RM Installation **Home Directory** "[RM Home Directory](#)" on page 158.
- The **Oracle Home Directory**, required for Oracle Database users:

### License Tab:

- The RM License Server Settings "[Setting the License Server](#)" on page 159.

### Security Tab:

- The name and location of the Security.dat file: "[The Location of the Database Password File](#)" on page 160.

## RM Home Directory



**CAUTION!** If this value is not set properly, you cannot launch other Dimensions RM tools from RM Manage.

**To check or set the RM Home Directory:**

- 1 In **RM Manage**, select **Workspace | Options**.
- 2 Click the **Mandatory** tab.
- 3 In **RM Home Directory**, if currently incorrectly set, enter the location of Dimensions RM or browse to the Dimensions RM installation directory.  
e.g., C:\Program Files\Open Text\Dimensions 25.2\RM
- 4 Click **Apply**.

**Oracle Users Must Set ORACLE\_HOME**

**When using RM with Oracle, ORACLE\_HOME** must be set to the Oracle installation directory. This value is stored in the registry and is used to determine the top-level installation directory of your company's Oracle RDBMS; this enables RM Manage to determine where the 'tnsnames.ora' file is located.



**CAUTION!** If this value is not set properly, you will not be able to see any database instances that are not local to the machine you are using.

**To check or set the Oracle Home Directory in RM Manage:**

- 1 In **RM Manage**, select **Workspace | Options**.
- 2 Click the **Mandatory** tab.
- 3 In **Oracle Home Directory**: if incorrectly set, enter the location of the Oracle Home directory.
- 4 Click **Apply**.

**Setting the License Server****NOTE**

**RM Manage** does not require a license for most functions:

In order to avoid licensing issues during setup, or at any time a License error is raised during the execution of RM Manage, please exit and run as administrator:

This also applies to the execution of class definition from the command line:  
bin\ClasDef.exe.

**To check or set the license server:**

- 1 **Right-click on RM Manage, and select Run as administrator from the context menu.**
- 2 In **RM Manage**, select **Workspace | Options**.
- 3 Select the **License** tab.
- 4 **License Tool:** Specifies which licensing application is used. Only **Open Text AutoPass Licensing** is supported.

- 5 License Type:** Specifies which license type is used. The following license types are available:
- **EVAL:** This license type indicates that Dimensions RM is running in evaluation mode.
  - **Named Users:** When selecting this license type, only named user licenses are requested. A named license is a license for a specific user. Other users cannot use that license. If a named license for this user is not available, login fails.
  - **Concurrent Users:** When selecting this license type, only concurrent user licenses are requested. Concurrent user licenses can be used by any user. If no concurrent license is available at the time of login, login fails.
  - **Named or Concurrent Users:** When selecting this license type, the login process first tries to request a named user license. If this fails, a concurrent user license is requested. If this also fails, login fails. with a license error.



#### NOTE

- If the organization has only named user licenses, select **Named Users** to reduce the waiting time. **Named or Concurrent Users** will send a second request (for a concurrent license) if a named license is not available.
- If you have only concurrent licenses, select **Concurrent Users** to reduce the waiting time. **Named or Concurrent Users** will always send two requests, as the first request for a named license always fails.

- 6 License Server:** Specifies the server on which the license tool runs. To change the server, type the name or IP address of the license server.
- 7 Limited Users:** Checking this box allows the Instance Administrator to add users with **Read Only Access** to any instance in the database. The setting for specific users will be available when a user is created or modified.
- Users may be added to existing groups and categories, but with read-only access to the data.
- The assignment of the limited license is standard: named or concurrent depending on the user assignment.
- 8** Click **Apply** to save changed license server settings.

## The Location of the Database Password File

The database password security file (`security.dat`) contains a security token and the encrypted database password for the database user ICADMIN.

If the default location of this file is changed, the location of the file location must also be changed as directed below..

#### To check or change the location of the security.dat file:

- 1 Right-click on RM Manage, and select Run as administrator from the context menu.**
- 2 In RM Manage, select Workspace | Options.**
- 3 Select the Security tab..**

- 4 In the **Security File** dialog box, if incorrectly set, type the full path to the security.dat file or browse to it. For example:  
C:\Program Files\Open Text\Dimensions 25.2\RM\security.dat
- 5 Click **OK**.

## Functions Available from RM Manage

The following sections describe the functions available to the **System Administrator** in RM Manage.

Access to RM Manage is only available to members if the **System Administrator group**. However, many actions available from RM Manage are available to both the **Instance Administrator** and the **System Administrator** from the Administration menu in Dimensions RM User Interface.

Initial Configuration of Dimensions RM must be completed in RM Manage. RM Manage must also be used to:

**Create the ICDBA account** (see "[Creating the ICDBA Account](#)" on page 161)

**Create new instances** (see "[Managing Instances](#)" on page 164)

**Backup and restore instances** (see "[Dimensions RM Backup](#)" on page 182, "[Restoring an Instance Account from a Backup](#)" on page 189, "[Backing Up Instances from the Command Line](#)" on page 196)

**Copying workflows to another class** (see "[Copying a Workflow to another Class](#)" on page 344)

**Schema deployment to other servers** (see "[Deploying the Instance Schema](#)" on page 324)


**Define new class types or Manage Class Types** (see "[Class Types](#)" on page 316)

All other Actions, including Category definition and management, Group and User Management, and continued schema modification, may be executed from the Dimensions RM Browser. by the Instance Administrator.

## Creating the ICDBA Account

The ICDBA account should be created once, in a database, and only once. The ICDBA account is used to execute all DBA functions. For details see [Database Accounts Used by Dimensions RM47](#).

**To create the ICDBA account:**

- 1 In **RM Manage**, 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.



**NOTE** The password is case sensitive.

- 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 Oracle account that you want to use, for example, SYS.
- 7 In the associated **Password** field, type the associated password for the account name.

## Oracle Tablespace

If Oracle is the database of choice, the ICDBA account is created, by default, in a new SERENA\_RM\_ADMIN tablespace for the ICDBA account and its size is set to 1024 MB. To

modify the size or create the ICDBA account in an existing tablespace, click the **Advanced** button. The dialog expands to display the advanced features.

**Create ICDBA account**

Create ICDBA account

Password: \*\*\*\*\*

Confirm Password: \*\*\*\*\*

Enter SYSDBA account password

Account Name: SYS

Password: \*\*\*

Buttons: Create, Cancel, Advanced <<

Tablespace option

Create in new tablespace

Create in existing tablespace

Administer Tablespaces...

Tablespace Name	Size (MB)	Avail (MB)
ARF	512.00	511.94
CAD	512.00	471.50
QRM	512.00	455.44
SYS_AUX	500.00	107.94
SYSTEM	650.00	106.00

Tablespace Size: 1024

Units:  MBytes  GBytes

- 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.

8 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 to change the ICDBA password before 180 days elapse using the RM Manage **Change Administrator Password** menu item, see "[Database Administrator Accounts](#)" on page 225.

## Managing Instances



**IMPORTANT!** New Instances need new permissions. Almost all user and group permissions should be managed by the Instance Administrator in RM Browser - but the Instance Administrator **first needs access to the instance.**

- 1 To create a new **Oracle Database Instance** see ["Creating an Instance with Oracle Databases" on page 164](#) and, if relevant, ["Using Advanced Options When Creating a New Instance with Oracle Databases" on page 172.](#)
- 2 To create a new instance using **MS SQL Server** see ["Creating a New Instance with MS SQL Server Databases" on page 173.](#)
- 3 to create a new **PostgreSQL Database Instance** see ["Creating a New Instance with PostgreSQL Databases" on page 175.](#)

**Once the new instance is created, please perform the following for all database types:**

- ["Adding a User to a Group" on page 212:](#) in order to add the Instance Administrator(s) to the Administrator group for the instance specified
- ["Setting Default Group Access" on page 218](#) in order to assign permissions to the Administrator group in this new instance.

### Creating an Instance with Oracle Databases

An instance is a work area where information is created and maintained. Dimensions RM provides users with the ability to create and delete instance accounts, backup and restore instances and administer user accounts.

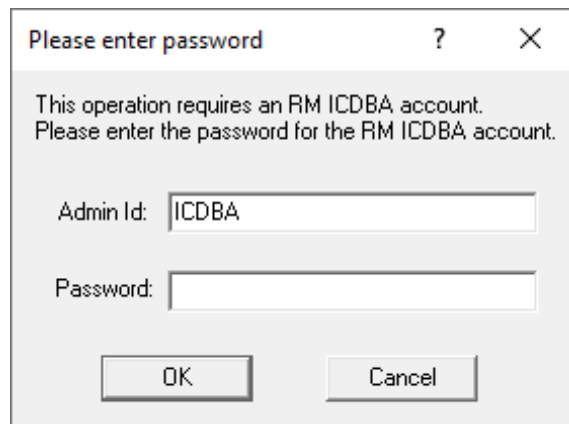


**IMPORTANT!**

- The ICDBA account (as explained in ["Creating the ICDBA Account" on page 161](#)) must exist before a new instance is created.

**To create an instance:**

- 1 In **RM Manage**, select the database in which you want to add the new instance.
- 2 Select **File | New Instance**, right-click the database and select **New Instance**.
- 3 The **Please enter password** dialog box opens. In the **Password** field, type the password for the Dimensions RM ICDBA account.



Please enter password ? X

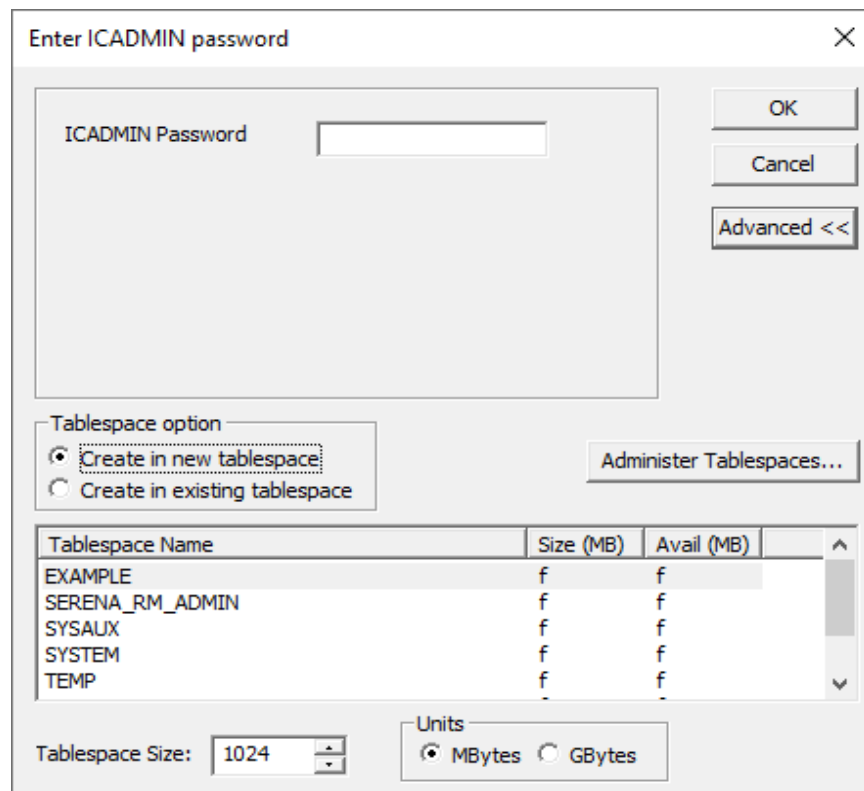
This operation requires an RM ICDBA account.  
Please enter the password for the RM ICDBA account.

Admin Id: ICDBA

Password:

OK Cancel

- 4 If the ICADMIN user has not yet been created, the **Enter ICADMIN password** dialog box opens.



Enter ICADMIN password X

ICADMIN Password

OK  
Cancel  
Advanced <<

Tablespace option

Create in new tablespace...  
 Create in existing tablespace

Administer Tablespaces...

Tablespace Name	Size (MB)	Avail (MB)
EXAMPLE	f	f
SERENA_RM_ADMIN	f	f
SYSAUX	f	f
SYSTEM	f	f
TEMP	f	f

Tablespace Size: 1024

Units  
 MBytes  GBytes

**Execute the following step in this dialog:**

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



**NOTE** The password is case sensitive.

- b Click **OK**.

- 5 The **Please Enter Instance Information** dialog box opens. Complete the following.

Please Enter Instance Information

Instance Name: TDRPOWER

Instance Password: [Masked]

Confirm Instance Password: [Masked]

Administrator Password: [Masked]

Confirm Administrator Password: [Masked]

Install instance tables      Set locale: English



Logon as administrator of this instance when finished      Show Password Rules


OK

Cancel

Advanced >>

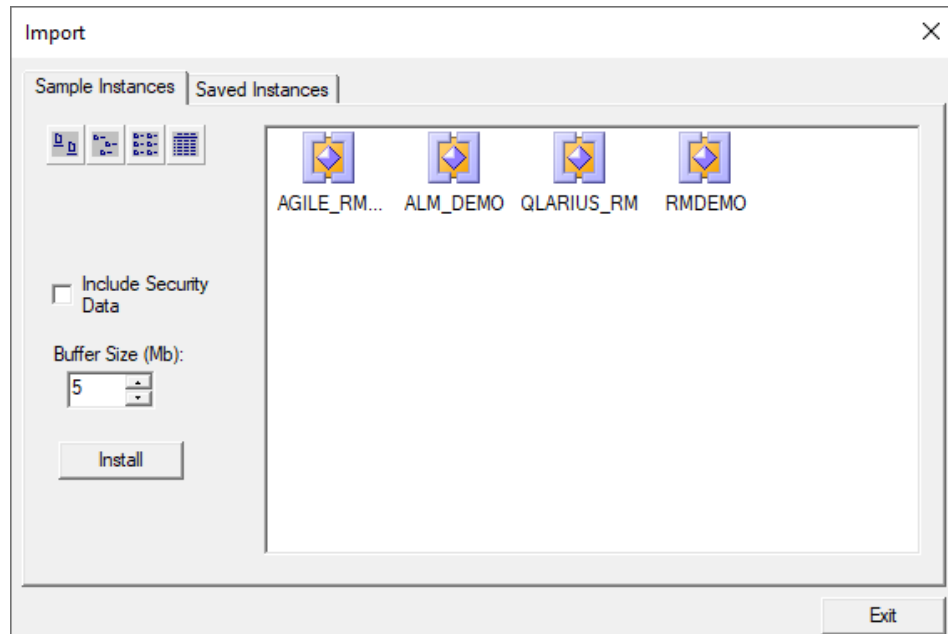
Oracle Only

Instance Information Dialog	
Field Name	Description
Instance Name 	Enter an instance name (for example, <b>MYINSTANCE</b> ). <b>CAUTION!</b> The instance name must follow the conventions specified in Section " <a href="#">Naming Conventions for Instances</a> " on page 28
Instance Password 	Enter an instance password (e.g., XyzzyZZY.42). This password is used by Dimensions RM to access Oracle. It is not a login password. <b>CAUTION!</b> Instance passwords cannot begin with a number. For example, 12345 causes an error; however, a12345 is accepted. Click <b>Show Password Rules</b> for a summary of the rules.
Confirm Instance Password	Re-enter the instance password.
Administrator Password	Enter a password for the Instance administrator account. This account has access only to this instance in RM Manage. The ID for this account is the instance name, with Admin appended, for example: MYINSTANCEAdmin  Historically, this account was used by the Instance Administrator to manage schema, groups and users in that instance. This functionality is now available in the browser, and security requirements have required that only individuals designated as System Administrators may access RM Manage directly.
Confirm Administrator Password	Re-enter the administrator password.
Install instance tables	<b>Selected:</b> When creating a new instance, the instance will be, initially, empty. <b>Cleared:</b> During the creation process, the Import dialog opens from which you can import a sample instance, a locally saved instance, or a backup.

Instance Information Dialog	
Field Name	Description
Set Locale	Set the Default Language for the Instance. This may be changed by individual users via RM Browser Settings.
<p>Ligon as administrator of this instance when finished.</p> 	<p><b>Selected:</b> Current user will be logged in as the RM Manage Instance Admin (e.g., MyinstanceAdmin).  <b>Cleared:</b> Recommended, you will remain logged in as the System Administrator.</p> <p>In either case, you must assign at least one user with the role of <b>Instance Administrator</b> to this instance.</p> <p>If no users have been created, please create one or two - once the Instance Administrator is created and assigned, they can take care of user creation from the user interface.</p> <ul style="list-style-type: none"> <li>▪ <a href="#">"Creating a New User" on page 206</a></li> <li>▪ <a href="#">"Adding a User to a Group" on page 212</a>: in order to add the Instance Administrator(s) to the Administrator group for the instance specified</li> <li>▪ <a href="#">"Setting Default Group Access" on page 218</a> in order to assign permissions to the Administrator group in this new instance.</li> </ul>

- 6 Click **OK**. The create operation runs.
- 7 **Tablespace Error** dialog boxes may open during instance creation to indicate that particular tables are not large enough. If this occurs, do the following for each **Tablespace Error** dialog box:
  - a Read and take note of the error message in the dialog box. You will need to refer to the values recommended here later.
  - b Click **Yes**. A **Resize Tablespace** dialog box opens.
  - c Increase the value in the **New Datafile Size** field by at least the amount recommended in [Step a](#).
  - d Click **Resize**. A **Resize** dialog box opens.
  - e In the **Resize** dialog box, click **Yes**.
  - f In the **Resize Tablespace** dialog box, click **Close**.
- 8 A Success dialog appears. Click **OK**.
- 9 If the option **Install instance tables** was selected on the **Please Enter Instance Information** dialog, all further steps are omitted.

**10** The **Import** dialog opens.



The **Import** dialog allows tables to be installed in the newly created instance. Do one of the following:

- **Do not install tables**—Click **Exit** without selecting any Instance files. You are done with this procedure. You can either remove the instance or install tables into it later.
- **Install a sample instance**—Select one of the sample instances from the **Sample Instances** tab:

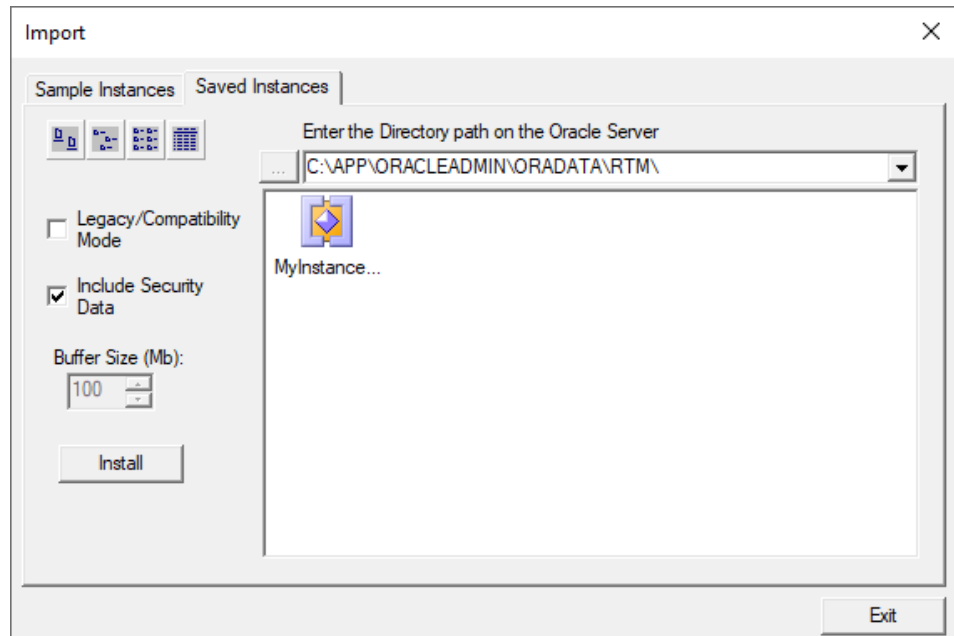
Instance	Description
ALM_DEMO	This sample instance provides classes and data for software requirements management, creating ALM applications.
QLARIUS_RM	This sample instance provides classes and data for an Insurance Company website and can be used in combination with the provided instance of Prototype Composer.
RMDEMO	This sample instance provides classes and data for requirement management projects.
AGILE_RMDEMO	This sample instance provides classes and data for requirement management projects in combination with Agile development.



**CAUTION!**

- Do NOT use any sample instance as a starting point for an actual production instance. They are useful for training, or for reproducing issues to be raised to support, but they carry a lot of history - better to start with a clean slate.




- **Install a saved instance or a backup** —Select the instance from the **Saved Instances** tab.



**NOTE** In Non-Legacy mode, you can only access backups that have been created with RM Manage. Backups copied to the server manually will not be available for selection.



**TIP**

- Instances displayed with an instance icon  contain data. Instances displayed with a class icon  contain only the instance schema.
- To view the modification date and size of the files, click the Details button .

- 11 Set the import options as needed:

Import Dialog	
Field	Description
Legacy/Compatibility Mode	<b>NOTE</b> Saved Instances tab only. Select this checkbox if you wish to import from a backup file that was created with RM 11.2.1 or older, or that was created in Legacy Mode with RM 11.2.2 or newer.
Security Data	Imports all the users in the backed up instance, as well as their permissions.
Buffer Size	<b>NOTE</b> Legacy Mode and Sample Instances tab only. This sets the temporary space available for the operation.

- 12 Click **Install**. The import operation runs.

- 13 When prompted, click **Yes** to view a log of the import operation, or **No** to exit without looking at the log.



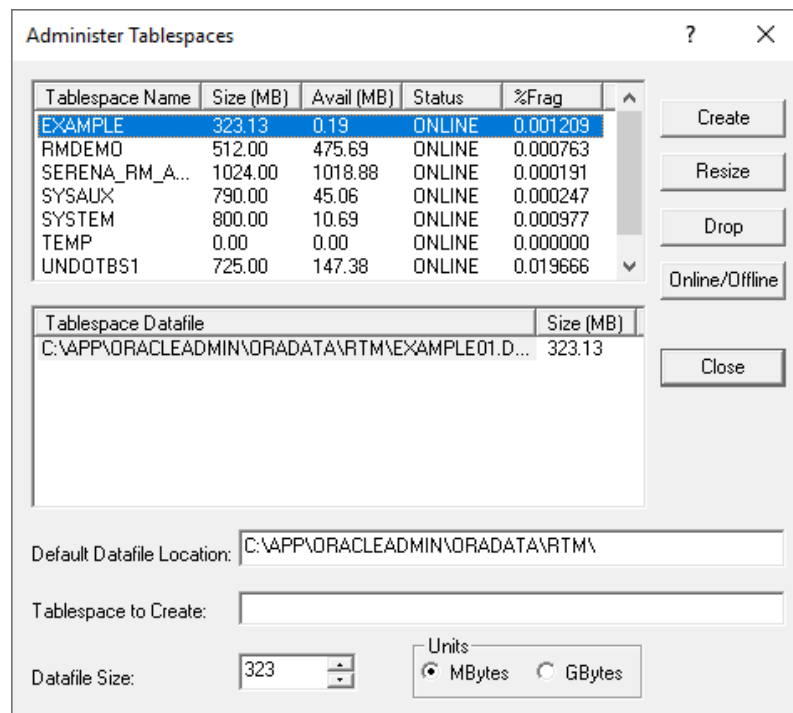
**TIP** The log file is saved in the directory where the backup was created. It has the same name as the instance, but with a .log extension instead of a .dmp extension. It also includes the letters "Imp" and a time stamp based upon the restore operation, e.g. *InstanceName\_ExpDate\_ExpTime\_Imp\_ImpDate\_ImpTime.log*



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

- 14 **Oracle Tablespace:** The default tablespace size for new instances is 512 MB. If this is not large enough to accommodate data contained in the instance that is being imported, you can resize the tablespace by using the **Administer Tablespaces** dialog box.

To resize an existing tablespace, highlight the database and select **Administer Tablespace**. The **Administer Tablespaces** dialog box opens.



**NOTE Administer Tablespace** is not available in Amazon Cloud mode. For further information, see chapter ["Using RM Manage within the Amazon Cloud"](#) on page 262.

- 15 Select a datafile size and click **Resize**. A prompt asks "Do you wish to resize an existing datafile?".
- 16 Click **Yes**.
- 17 Click **Close**.

## Using Advanced Options When Creating a New Instance with Oracle Databases

The **Advanced** button on the **Please Enter Instance Information** dialog box provides access to advanced tablespace options for new instances, such as inserting the new instance into a pre-existing tablespace and changing the default tablespace size.

### To use advanced options:

- 1 In the **Please Enter Instance Information** dialog box, click **Advanced**. The dialog box expands to show advanced options.

Tablespace Name	Size (MB)	Avail (MB)
AGILE_RMDEMO	512.00	511.00
RMDEMO	512.00	472.69
SERENA_RM_ADMIN	1024.00	1018.00
SYSAUX	644.00	93.69
SYSTEM	838.00	123.69

- 2 To insert the new instance into a pre-existing tablespace, click **Create in existing tablespace**, and then select a tablespace from the list. Otherwise, the instance will be created in a new tablespace.
- 3 If you choose to create the instance in a new tablespace, you can change its size from the default size of 160 MB by editing the value in the **Tablespace Size** list box and selecting a **Units** option (megabytes or gigabytes).
- 4 If you choose to create the instance in an existing tablespace and you want to adjust the size of that tablespace to ensure it has enough space to hold the new instance, click **Administer Tablespaces** to access the tablespace management features (described in "[Administering Tablespaces](#)" on page 237).


## Creating a New Instance with MS SQL Server Databases

An instance is a work area where information is created and maintained. Dimensions RM provides you with the ability to create and delete instance accounts, backup and restore instances and administer user accounts.



**IMPORTANT!** Before you can create a Dimensions RM instance, you must have configured MS SQL Server and created a database. For further information on configuration of MS SQL Server and creating a database instance, see the *"Dimensions RM Installation Guide"*, chapter *"Installing and Configuring MS SQL Server"*.

### To create a new instance:

- 1 In **RM Manage**, select the database in which you want to add the new instance.
- 2 Select **File | New Instance**, click the **New Instance** button , or right-click the database and select **New Instance**.
- 3 The **Please enter password** dialog box opens. In the **Password** field, type the password for the Dimensions RM ICDBA account.



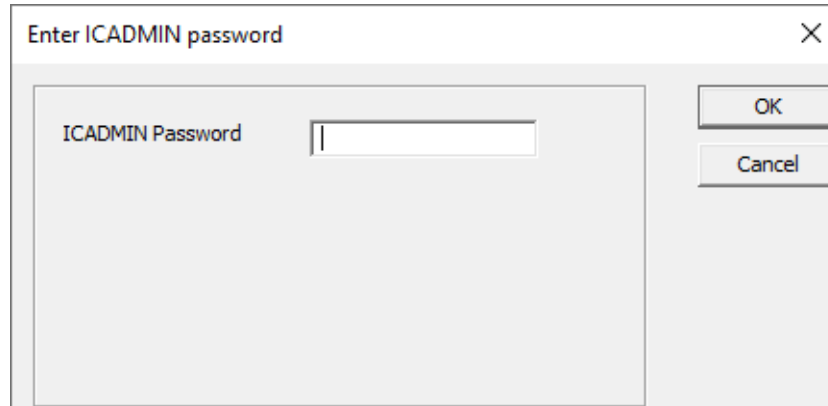

### IMPORTANT!

- You must ensure that you create the ICDBA account (as explained in ["All other Actions, including Category definition and management, Group and User Management, and continued schema modification, may be executed from the Dimensions RM Browser. by the Instance Administrator."](#) on page 161) and associated password before assigning the password to ICADMIN. There is no software check to ensure that this has been done in the correct order.
- When creating the ICADMIN database account, Dimensions RM automatically generates a new `security.dat` file. The old version of this file is renamed and retained as a backup.

If the ICADMIN user has not been created, the **Enter ICADMIN password** dialog box opens.

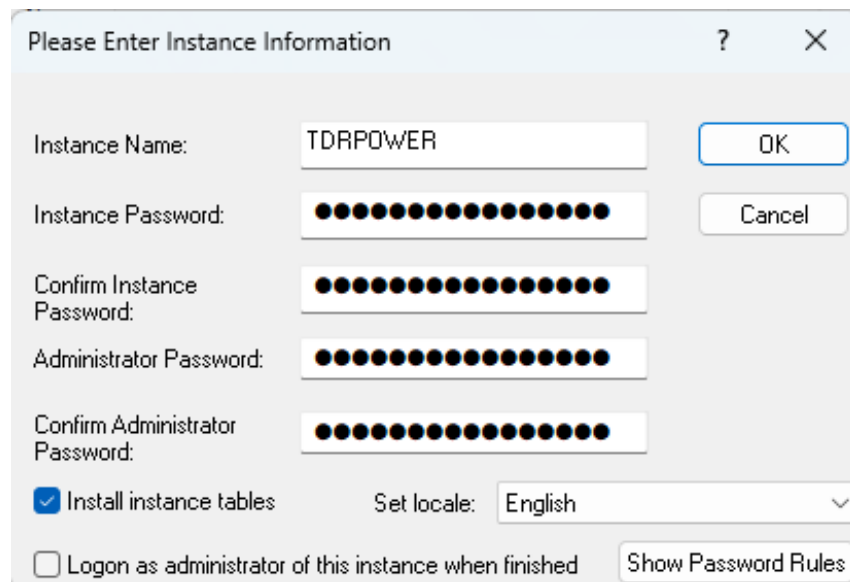
**Execute the following steps in this dialog:**


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



**NOTE** The password is case sensitive.

- b Click **OK**.
- 4 The **Please Enter Instance Information** dialog box opens. Complete the following fields as needed.




Please Enter Instance Information Dialog	
Field	Description
Instance Name	Enter an instance name (for example, MYINSTANCE).
	<b>CAUTION!</b> The instance name must follow the conventions specified in chapter "Naming Conventions for Instances" on page 28.
Instance Password	Enter an instance password (for example, MYINSTANCE). This password is used by Dimensions RM to access MS SQL Server. RM users do not use it directly in Dimensions RM.  <b>NOTE</b> Instance passwords cannot begin with a number. For example, 12345 causes an error; however, a12345 is accepted. Click <b>Show Password Rules</b> for a summary of the rules.
Confirm Instance Password	Re-enter the instance password.
Administrator Password	Enter a password for the Instance administrator account. This account has access only to this instance in RM Manage. The ID for this account is the instance name, with Admin appended, for example: MYINSTANCEAdmin  Historically, this account was used by the Instance Administrator to manage schema, groups and users in that instance. This functionality is now available in the browser, and security requirements have required that only individuals designated as System Administrators may access RM Manage directly.
Confirm Administrator Password	Re-enter the administrator password.
Install instance tables	With MS SQL Server, this option can't be modified. You will always create an empty instance.
Set Locale	Set the Default Language for the Instance; this may be changed by individual users via RM Browser Settings. Available languages include: Chinese, English, German, Japanese, Spanish, and Brazilian Portuguese.
Logon as administrator of this instance when finished	Upon completion of the create operation, opens the new instance and logs you in as the administrator.

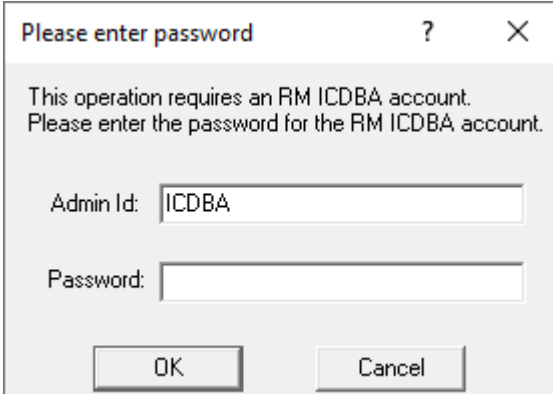
- 5 Click **OK**. The create operation runs.

## Creating a New Instance with PostgreSQL Databases

An instance is a work area where information is created and maintained. Dimensions RM provides you with the ability to create and delete instance accounts, backup and restore instances and administer user accounts.

**To create a new instance:**

- 1 In **RM Manage**, select the database in which you want to add the new instance.
- 2 Select **File | New Instance**, click the **New Instance** button , or right-click the database and select **New Instance**.
- 3 The **Please enter password** dialog box opens. In the **Password** field, type the password for the Dimensions RM ICDBA account.



Please enter password ? X

This operation requires an RM ICDBA account.  
Please enter the password for the RM ICDBA account.

Admin Id:

Password:

OK Cancel

**IMPORTANT!**

- You must ensure that you create the ICDBA account (as explained in ["All other Actions, including Category definition and management, Group and User Management, and continued schema modification, may be executed from the Dimensions RM Browser, by the Instance Administrator."](#) on page 161) and associated password before assigning password to ICADMIN. There is no software check to ensure that this has been done in the correct order.
- When creating the ICADMIN database user, Dimensions RM automatically generates a new `security.dat` file. The old version of this file is renamed and retained as a backup.

If the ICADMIN user has not been created, the **Enter ICADMIN password** dialog box opens.



**Execute the following steps in this dialog:**


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



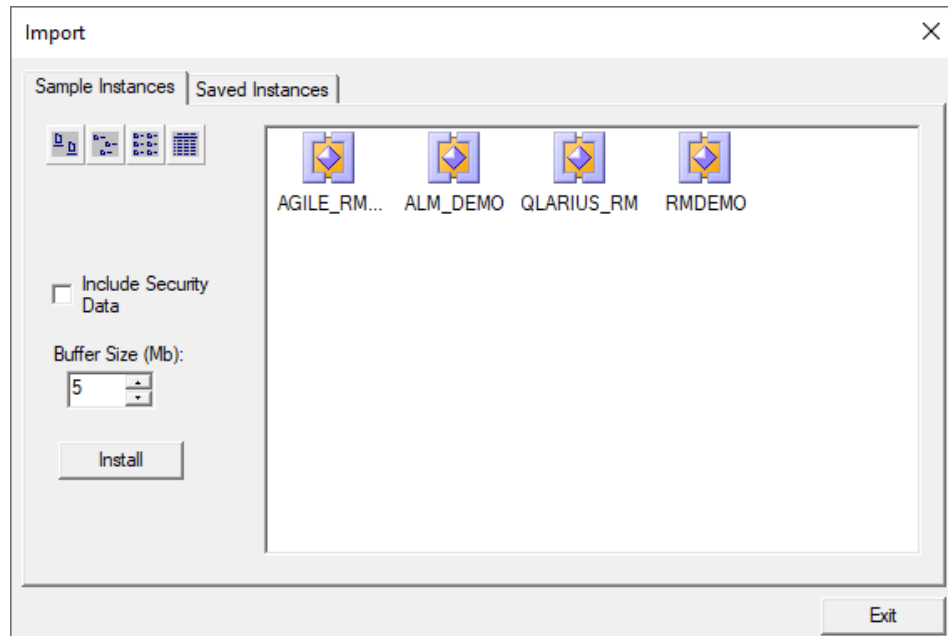
**NOTE** The password is case sensitive.

- b Click **OK**.
- 4 The **Please Enter Instance Information** dialog box opens. Complete the following fields as needed.

Instance Information Dialog	
Field Name	Description
Instance Name 	Enter an instance name (for example, <b>MYINSTANCE</b> ). <b>CAUTION!</b> The instance name must follow the conventions specified in Section <a href="#">"Naming Conventions for Instances"</a> on page 28
Instance Password 	Enter an instance password (e.g., XyzzyZZY.42). This password is used by Dimensions RM to access Oracle. It is not a login password. <b>CAUTION!</b> Instance passwords cannot begin with a number. For example, 12345 causes an error; however, a12345 is accepted. Click <b>Show Password Rules</b> for a summary of the rules.
Confirm Instance Password	Re-enter the instance password.
Administrator Password	Enter a password for the Instance administrator account. This account has access only to this instance in RM Manage. The ID for this account is the instance name, with Admin appended, for example: MYINSTANCEAdmin  Historically, this account was used by the Instance Administrator to manage schema, groups and users in that instance. This functionality is now available in the browser, and security requirements have required that only individuals designated as System Administrators may access RM Manage directly.
Confirm Administrator Password	Re-enter the administrator password.
Install instance tables	<b>Selected:</b> When creating a new instance, the instance will be, initially, empty. <b>Cleared:</b> During the creation process, the Import dialog opens from which you can import a sample instance, a locally saved instance, or a backup.

Instance Information Dialog	
Field Name	Description
Set Locale	Set the Default Language for the Instance. This may be changed by individual users via RM Browser Settings.
<p>Logon as administrator of this instance when finished.</p> 	<p><b>Selected:</b> Current user will be logged in as the RM Manage Instance Admin (e.g., MyinstanceAdmin).  <b>Cleared:</b> Recommended, you will remain logged in as the System Administrator.</p> <p>In either case, you must assign at least one user with the role of <b>Instance Administrator</b> to this instance.</p> <p>If no users have been created, please create one or two - once the Instance Administrator is created and assigned, they can take care of user creation from the user interface.</p> <ul style="list-style-type: none"> <li>▪ <a href="#">"Creating a New User" on page 206</a></li> <li>▪ <a href="#">"Adding a User to a Group" on page 212</a>: in order to add the Instance Administrator(s) to the Administrator group for the instance specified</li> <li>▪ <a href="#">"Setting Default Group Access" on page 218</a> in order to assign permissions to the Administrator group in this new instance.</li> </ul>

- 5 Click **OK**. The create operation runs.
- 6 **Tablespace Error** dialog boxes may open during instance creation to indicate that particular tables are not large enough. If this occurs, do the following for each **Tablespace Error** dialog box:
  - a Read and take note of the error message in the dialog box. You will need to refer to the values recommended here later.
  - b Click **Yes**. A **Resize Tablespace** dialog box opens.
  - c Increase the value in the **New Datafile Size** field by at least the amount recommended in [Step a](#).
  - d Click **Resize**. A **Resize** dialog box opens.
  - e In the **Resize** dialog box, click **Yes**.
  - f In the **Resize Tablespace** dialog box, click **Close**.
- 7 A Success dialog appears. Click **OK**.
- 8 If the option **Install instance tables** was selected on the **Please Enter Instance Information** dialog, all further steps are omitted.

9 The **Import** dialog opens.

The **Import** dialog allows tables to be installed in the newly created instance. Do one of the following:

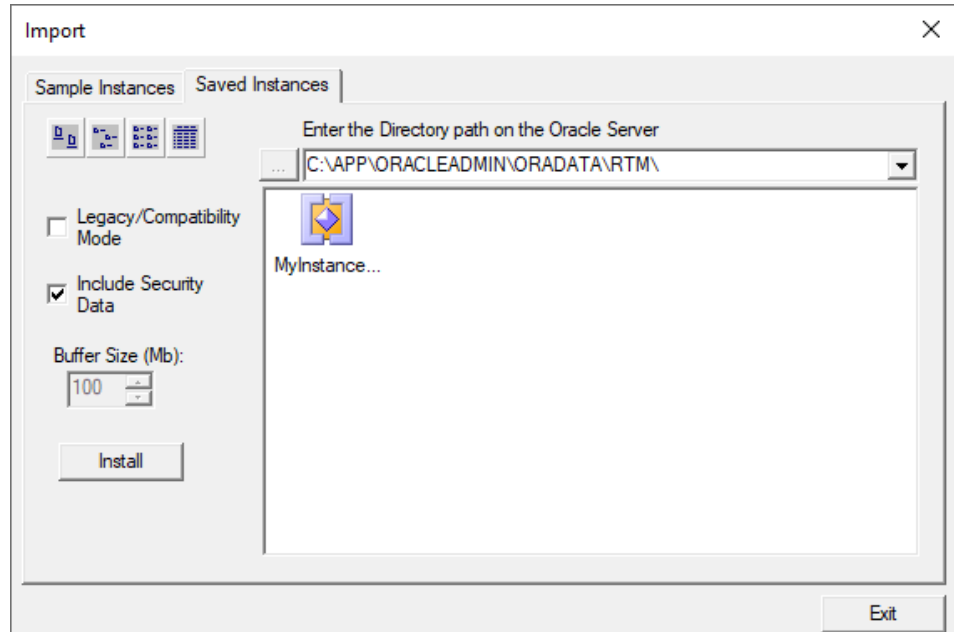
- **Do not install tables**—Click **Exit** without selecting any files. You are done with this procedure. You can either remove the instance or install tables into it later.
- **Install a sample instance**—Select one of the sample instances from the **Sample Instances** tab:

Instance	Description
ALM_DEMO	This sample instance provides classes and data for software requirements management, creating ALM applications.
QLARIUS_RM	This sample instance provides classes and data for an Insurance Company website and can be used in combination with the provided instance of Prototype Composer.
RMDEMO	This sample instance provides classes and data for requirement management projects.
AGILE_RMDEMO	This sample instance provides classes and data for requirement management projects in combination with Agile development.




**CAUTION!**

- Do NOT use any sample instance as a starting point for an actual production instance.

- **Install a saved instance**—Select the instance from the **Saved Instances** tab.



**TIP**

- Instances displayed with an instance icon  contain data. Instances displayed with a class icon  contain only the instance schema.
- To view the modification date and size of the files, click the Details button .

- 10 Set the import options as needed:

Import Dialog	
Field	Description
Include Security Data	Imports all the users in the backed up instance, as well as their permissions.


- 11 Click **Install**. The import operation runs.
- 12 When prompted, click **Yes** to view a log of the import operation, or **No** to exit without checking the log.

## Changing the Instance Password

This section describes how to change an instance password. If your instance password has been changed without using RM Manage, see chapter "[Updating the Instance Password](#)" on page 182. See also "[Database Administrator Accounts](#)" on page 225 and "[Changing an Instance Administrator Password](#)" on page 231.

**To change the instance password:**


- 1 In **RM Manage**, select the instance for which you want to change the password.

- 2 Select **File | Change Instance Password**, click the **Change Instance Password** button , or right-click the instance and select **Change Instance Password**.
- 3 Enter your system administrator password.
- 4 Click **OK**. This opens the **Change Instance Password/Instance Admin Password** dialog.
- 5 Select the **Retain the current InstanceAdmin password** option. This disables all text boxes and options related to the instance admin password.
- 6 Type the new password into the **Instance (DB) Password** box.
- 7 Re-type the password into the **Confirm Instance (DB) Password** box.
- 8 Click **OK**.

## Updating the Instance Password

This section describes how to update the password record if the database password for the instance has been changed without using RM Manage. For a regular password change, see chapter "[Changing the Instance Password](#)" on page 181. See also "[Database Administrator Accounts](#)" on page 225 and "[Changing an Instance Administrator Password](#)" on page 231.

### To update the instance password:

- 1 In **RM Manage**, select the instance for which you want to change the password.
- 2 Select **File | Change Instance Password**, click the **Change Instance Password** button , or right-click the instance and select **Change Instance Password**.
- 3 Enter your system administrator password.
- 4 Click **OK**. This opens the **Change Instance Password/Instance Admin Password** dialog.
- 5 Select the **Retain the current InstanceAdmin password** option. This disables all text boxes and options related to the instance admin password.
- 6 Select the **Apply DB password** option. This disables the **Confirm Instance (DB) Password** box.
- 7 Type the new password into the **Instances (DB) Password** box.
- 8 Click **OK**.

## Dimensions RM Backup

When using an Oracle Database see: "[Backing Up an Instance Account under Oracle](#)" on page 183

When using MS SQL Server see: "[Backing Up an Instance Account under MS SQL Server](#)" on page 185

When using PostgreSQL: ["Backing Up an Instance Account under PostgreSQL" on page 187](#)

### **Backing Up an Instance Account under Oracle**



**IMPORTANT!** When you back up an instance account, you back up an Oracle account containing:

- Oracle tables holding the entire Dimensions RM schema metadata.
- Other Oracle tables holding the actual requirement data.



#### **CAUTION!**

Before beginning the backup, you need to ensure that no users are accessing Dimensions RM while instance data is secured. To ensure this, stop these services:

- **Dimensions RM Common Tomcat**
- **Dimensions RM Pool Manager**
- **Dimensions RM E-Mail Notification Service**

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



**NOTE** When running in Amazon Cloud mode, backups can only be created in legacy mode. For further information, see chapter ["Using RM Manage within the Amazon Cloud" on page 262](#).

#### **To back up an instance account:**

- 1 Ensure that no users are accessing Dimensions RM.
- 2 It is advisable to first place each instance account offline, see ["Placing an Instance Account Offline" on page 204](#).
- 3 In **RM Manage** please select the instance to be backed up.
- 4 Select **File | Backup/Restore Instance Account**.
- 5 If prompted, enter your ICDBA password and click **OK**.
- 6 The Backup/Restore Instance dialog appears. Enter the path intended to hold backups, as well as the file name.

#### **Backup/Restore Instance Dialog**

Field	Description
Legacy/Compatibility Mode	Formats the backup so that can be imported on systems that only support legacy mode.
Directory Path	This field is automatically populated with the last modified server directory path for the selected instance. Edit the path as needed.  <b>NOTE</b> This field is not available in Legacy Mode.

Backup/Restore Instance Dialog	
Field	Description
File Name	<p>This field is automatically populated with a name for the backup file. The name is based upon the database or instance name and the current date and time. Edit this name as needed.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>▪ <b>Legacy Mode:</b> The path to the Saved Projects directory of the RM installation is prepended to the file name.</li> </ul>
...	<p>Opens a dialog to select the backup file.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>▪ <b>Normal Mode:</b> Enter the dump file name as described for the <b>File Name</b> field.</li> <li>▪ <b>Legacy Mode:</b> This opens a file selection dialog to choose a file name for saving to backup.</li> </ul>
Security Data	<p>Exports all the users that have been assigned to this instance, as well as their permissions, so that they may be imported into another instance.</p>
Buffer Size	<p><b>NOTE</b> Legacy Mode only.</p> <p>This sets the temporary space available for the operation. The default, and maximum, buffer size is 100MB. You can adjust the amount if needed.</p>

- 7 Click the **Backup** button. The backup operation runs.
- 8 Click **Display Log** to view a log of the backup operation.



**TIP** The log file is saved in the directory where the backup was created. It has the same file name, but with a .log extension.

- 9 Restart the following services:
  - Dimensions RM Pool Manager
  - Dimensions RM Common Tomcat
  - Dimensions RM E-Mail Notification Service (if it ran before)

## Backing Up an Instance Account under MS SQL Server



### PRIVILEGES

Before beginning the backup, ensure that MS SQL Server can access the directory you want to write the backup file to.

#### To grant write access to a directory, do the following:

- 1 In Windows Explorer, right-click the folder you want to grant write access to.
- 2 Select **Properties** from the shortcut menu to open the **Properties** dialog.
- 3 Select the **Security** tab.
- 4 Click **Edit...** to open the **Permissions** dialog.
- 5 Click **Add...** This opens the **Select Users or Groups** dialog.
- 6 Enter NT SERVICE\MSSQLSERVER and click **OK**.
- 7 In the Allow column, select the **Full control** option and click **OK**.
- 8 Click **OK** to close the **Properties** dialog.



### IMPORTANT!

When you back up an instance account, you back up the whole MS SQL Server database holding that instance account. Each instance account contains:

- Database tables holding the entire Dimensions RM schema metadata.
- Other database tables holding the actual requirement data.



### CAUTION!

Before beginning the backup, you need to ensure that no users are accessing Dimensions RM while instance data is secured. To ensure this, stop these services:

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

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



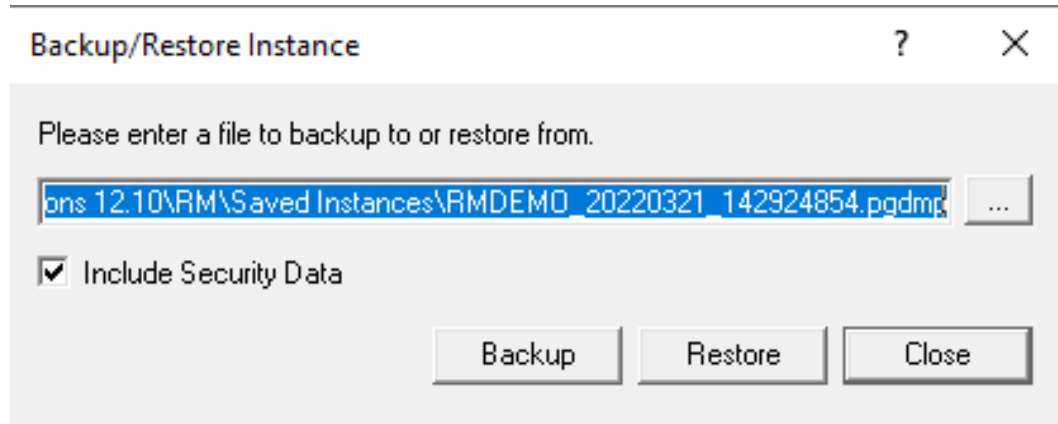
### NOTE


- The backup will always be created on the database server.
- When running in Amazon Cloud mode, backups can only be created in legacy mode. For further information, see chapter ["Using RM Manage within the Amazon Cloud"](#) on [page 262](#).

#### To back up an instance account:

- 1 Ensure that no users are accessing Dimensions RM.

- 2 It is advisable to first place each instance account offline, see "Placing an Instance Account Offline" on page 204.
- 3 In **RM Manage**, right-click the database you want to back up and select **Backup/Restore Database** from the shortcut menu.
- 4 If prompted, enter the ICDBA password and click **OK**.
- 5 The Backup/Restore Instance dialog appears. Complete the following fields as needed.



Backup/Restore Instance Dialog	
Field	Description
File Name	<p>This field is automatically populated with a name for the backup file. The name is based upon the database name and the current date and time. Edit this name as needed.</p> <ul style="list-style-type: none"> <li>▪ <b>Local mode:</b> The path to the Saved Instances directory of the RM installation is prepended to the file name.</li> <li>▪ <b>Remote mode:</b> The location is relative to the MS SQL Server directory path.</li> </ul> <p> <b>NOTE</b> You can manually enter the name of the BAK file.</p>
Remote file location	Enable this option if Dimensions RM server and MS SQL Server run on different machines.
...	Opens a dialog to select the backup file. This button is only available when the <b>Remote file location</b> option is turned off.

- 6 Click the **Backup** button. The backup operation runs.
- 7 Click **Display Log** to view a log of the backup operation.



**TIP** 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 upon the backup operation, e.g. *InstanceName\_ExpDate\_ExpTime\_Exp.log*

- 8 Restart the following services:
  - Dimensions RM Pool Manager
  - Dimensions RM Common Tomcat
  - Dimensions RM E-Mail Notification Service (if it ran before)

### **Backing Up an Instance Account under PostgreSQL**



**IMPORTANT!** When you back up an instance account, you back up an PostgreSQL account containing:

- Database tables holding the entire Dimensions RM schema metadata.
- Other database tables holding the actual requirement data.



#### **CAUTION!**

Before beginning the backup, you need to ensure that no users are accessing Dimensions RM while instance data is secured. To ensure this, stop these services:

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

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

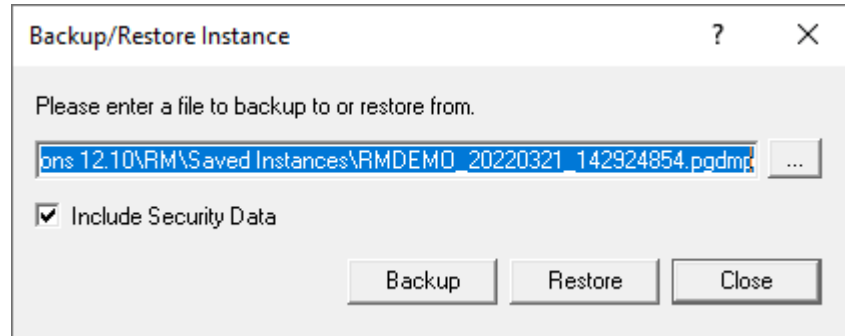



**NOTE** The backup will always be created on the database server.

#### **To back up an instance account:**

- 1 Ensure that no users are accessing Dimensions RM.
- 2 It is advisable to first place each instance account offline, see ["Placing an Instance Account Offline" on page 204](#).
- 3 In **RM Manage**, select the instance you want to back up.
- 4 Select **File | Backup/Restore Instance Account**.
- 5 If prompted, enter your administrator password and click **OK**.

- 6 The Backup/Restore Instance dialog appears. Complete the following fields as needed.



Backup/Restore Instance Dialog	
Field	Description
File Name	<p>This field is automatically populated with a name for the backup file. The name is based upon the database name and the current date and time. Edit this name as needed.</p> <ul style="list-style-type: none"> <li>▪ <b>Local mode:</b> The path to the Saved Instances directory of the RM installation is prepended to the file name.</li> <li>▪ <b>Remote mode:</b> The location is relative to the MS SQL Server directory path.</li> </ul> <p> <b>NOTE</b> You can manually enter the name of the BAK file.</p>
Include 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 instance.
...	Opens a dialog to select the backup file. This button is only available when the <b>Remote file location</b> option is turned off.

- 7 Click the **Backup** button. The backup operation runs.
- 8 Click **Display Log** to view a log of the backup operation.



**TIP** 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 upon the backup operation, e.g. *InstanceName\_ExpDate\_ExpTime\_Exp.log*

- 9 Restart the **Dimensions RM E-Mail Service** service.
- 10 Restart the following services:
- Dimensions RM Pool Manager
  - Dimensions RM Common Tomcat
  - Dimensions RM E-Mail Notification Service (if it ran before)
  -

## Restoring an Instance Account from a Backup

### Restoring an Instance Account under Oracle



**IMPORTANT!** When you back up an instance account, you back up an Oracle account containing:

- Oracle tables holding the entire Dimensions RM schema metadata.
- Other Oracle tables holding the actual requirement data.



#### CAUTION!

Before restoring the backup, you need to ensure that no users are accessing Dimensions RM while instance data is secured. To ensure this, stop these services:

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

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



**NOTE** When running in Amazon Cloud mode, backups can only be restored in legacy mode. For further information, see chapter "[Using RM Manage within the Amazon Cloud](#)" on page 262.

#### To restore an instance account from a backup using the RM Manage interface:

- 1 Check that the instance you wish to restore has (Current) next to its name. If this is not the case then you will first need to run the **Convert Database** command on the database and its instance accounts before performing the instance account restores. To convert the instance see chapter "[Converting Database and Instances](#)" on page 201.
- 2 In **RM Manage**, select the instance you want to restore.
- 3 Select **File | Backup/Restore Instance Account**.

- 4 The Backup/Restore Instance dialog appears. Complete the following fields as needed.

### Backup/Restore Instance Dialog

Field	Description
Legacy/Compatibility Mode	Select this check box if you wish to restore from a backup file that was created in Legacy Mode with RM 12.5.1 or newer.
Oracle Directory Path	This field is automatically populated with the last modified server directory path for the selected instance. Edit the path as needed.  <b>NOTE</b> This field is not available in Legacy Mode.
File Name	Enter the name of the file to restore from, or click ... to select one.  <ul style="list-style-type: none"> <li> <b>Normal Mode:</b> The file location is relative to the Oracle directory path.  <b>NOTE</b> You can manually enter the name of the DMP file instead of selecting from those of the dialog. </li> <li> <b>Legacy Mode:</b> The path to the Saved Projects directory of the RM installation is prepended to the file name. </li> </ul>
...	Opens a dialog to select the backup file.  <ul style="list-style-type: none"> <li> <b>Normal Mode:</b> The dialog contains the DMP file names available on the server.  <b>NOTE</b> You can only see the DMP files that were made from the currently selected instance. </li> <li> <b>Legacy Mode:</b> Opens a file selection dialog to choose the backup to restore. You can choose backup files from any available location. </li> </ul>

Backup/Restore Instance Dialog	
Field	Description
Security Data	Imports all the users in the backed-up instance, as well as their permissions.
Buffer Size	<p><b>NOTE</b> Legacy Mode only.</p> <p>This sets the temporary space available for the operation. The default, and maximum, buffer size is 100MB. You can adjust the amount if needed.</p>

- 5 Click **Restore**. The restore operation runs.



#### NOTES

- **Normal Mode only:** When restoring an instance, the **Please enter the from user** dialog may show.
  - **From User:** Enter the RM instance name as it was on the system from which the backup was created.
  - **Tablespace:** Enter the tablespace as it was on the system from which the backup was created. In most cases, the tablespace is identical with the text entered in **From User**.
- The existing tablespace may not be large enough to accommodate the data contained in the instance that is being restored. In this case, you will be asked if you would like to resize the tablespace before continuing. The process of resizing the tablespace is discussed in "[Resizing a Tablespace](#)" on page 239.

- 6 Click **Display Log** to view a log of the backup operation.



**NOTE** When importing in Legacy mode, you might receive these error messages:

- ORA-39082 "... created with compilation warnings"
- ORA-39083: Object type JOB failed to create with error

You can safely ignore these errors.



**TIP** 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 "Imp" and a time stamp based upon the restore operation, e.g. *InstanceName\_ExpDate\_ExpTime\_Imp\_ImpDate\_ImpTime.log*

- 7 Restart the following services:
- Dimensions RM Pool Manager
  - Dimensions RM Common Tomcat
  - Dimensions RM E-Mail Notification Service (if it ran before)

## Restoring an Instance Account under MS SQL Server



### IMPORTANT!

- When you back up an instance account, you back up the whole MS SQL Server database holding that instance account. Each instance account contains:
  - Database tables holding the entire Dimensions RM schema metadata.
  - Other database tables holding the actual requirement data.
- The backup file to import **must** be located on the database server.



### CAUTION!

Before restoring the backup, you need to ensure that no users are accessing Dimensions RM while instance data is secured. To ensure this, stop these services:

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

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



**NOTE** When running in Amazon Cloud mode, backups can only be restored in legacy mode. For further information, see chapter ["Using RM Manage within the Amazon Cloud"](#) on page 262.

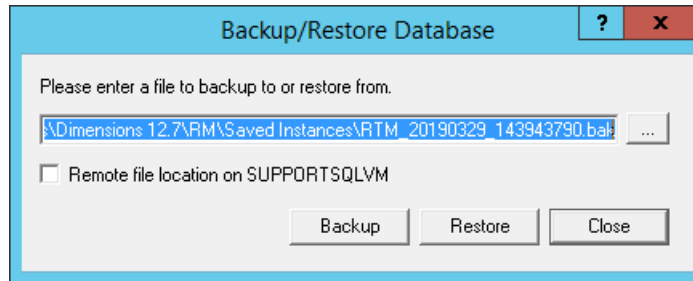
### To restore an instance account from a backup using the RM Manage interface:


- 1 In **RM Manage**, right-click the database you want to restore and select **Backup/Restore Database** from the shortcut menu.



**CAUTION!** Restoring a database will overwrite all RM instances of that database.

- If requested, enter the password for the ICDBA user and click **OK**. This opens the **Backup/Restore Database** dialog.



Backup/Restore Database Dialog	
Field	Description
File Name	<p>Enter the name of the file to restore from, or click ... to select one.</p> <ul style="list-style-type: none"> <li>▪ <b>Local mode:</b> The path to the Saved Instances directory of the RM installation is prepended to the file name.</li> <li>▪ <b>Remote mode:</b> The file location is relative to the MS SQL Server directory path. Use the Remote mode if Dimensions RM server and MS SQL Server run on different machines.</li> </ul> <p> <b>NOTE</b> You can manually enter the name of the BAK file.</p>
Remote file location	Enable this option if Dimensions RM server and MS SQL Server run on different machines.
...	Opens a file selection dialog to choose the backup to restore. This button is only available when the <b>Remote file location</b> option is turned off.

- Click **Restore**. The restore operation runs.



**CAUTION!** Restoring a database will overwrite all RM instances of that database.



**NOTES**

When restoring an instance, the **Enter ICADMIN password** dialog may show. Then, do the following:

- Enter the password for the ICADMIN user into the **ICADMIN Password** box.
- Click **OK**.

- Verify that the restore of the database completed without errors.
- Restart the following services:
  - Dimensions RM Pool Manager
  - Dimensions RM Common Tomcat

- Dimensions RM E-Mail Notification Service (if it ran before)

### **Restoring an Instance Account under PostgreSQL**



**IMPORTANT!** When you back up an instance account, you back up an PostgreSQL account containing:

- Database tables holding the entire Dimensions RM schema metadata.
- Other database tables holding the actual requirement data.



#### **CAUTION!**

Before restoring the backup, you need to ensure that no users are accessing Dimensions RM while instance data is secured. To ensure this, stop these services:

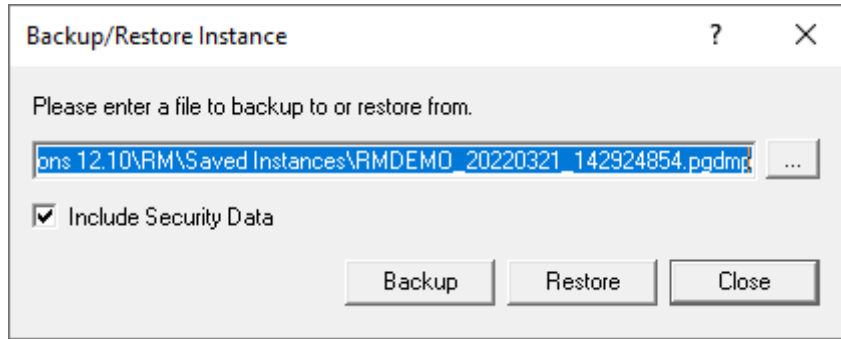
- Dimensions RM Common Tomcat
- Dimensions RM Pool Manager
- Dimensions RM E-Mail Notification Service



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

#### **To restore an instance account from a backup using the RM Manage interface:**

- 1** Check that the instance you wish to restore has (Current) next to its name. If this is not the case (for example it has a suffix of (VRM2010 R1 GA)), then you will first need to run the **Convert Database** command on the database and its instance accounts before performing the instance account restores. To convert the instance see chapter "[Converting Database and Instances](#)" on page 201.
- 2** In **RM Manage**, select the instance you want to restore.
- 3** Select **File | Backup/Restore Instance Account**.

- 4 The Backup/Restore Instance dialog appears. Complete the following fields as needed.



Backup/Restore Instance Dialog	
Field	Description
File Name 	Enter the name of the file to restore from, or click ... to select one. <ul style="list-style-type: none"> <li> <b>Normal Mode:</b> The file location is relative to the Oracle directory path.                             <p><b>NOTE</b> You can manually enter the name of the DMP file instead of selecting from those of the dialog.</p> </li> <li> <b>Legacy Mode:</b> The path to the Saved Projects directory of the RM installation is prepended to the file name.                             </li> </ul>
... 	Opens a dialog to select the backup file. <ul style="list-style-type: none"> <li> <b>Normal Mode:</b> The dialog contains the DMP file names available on the server.                             <p><b>NOTE</b> You can only see the DMP files that were made from the currently selected instance.</p> </li> <li> <b>Legacy Mode:</b> Opens a file selection dialog to choose the backup to restore. You can choose backup files from any available location.                             </li> </ul>
Include Security Data	Imports all the users in the backed-up instance, as well as their permissions.

- 5 Click **Restore**. The restore operation runs.
- 6 Click **Display Log** to view a log of the backup operation.
- 7 Restart the following services:
- Dimensions RM Pool Manager
  - Dimensions RM Common Tomcat
  - Dimensions RM E-Mail Notification Service (if it ran before)

## Backing Up Instances from the Command Line

In addition to using the **Backup/Restore Instance Account** option in RM Manage, you can back up an instance from the command line. The security information for the instance is automatically included in the backup.



**NOTE** Instances cannot be restored using the command line. You must use the RM Manage tool to restore a backed-up instance, regardless of how the backup file was created.

The following table describes the backup command line parameters:

Parameter	Description
icmanage	If <RM Install Dir>\bin is not specified in your PATH environment variable, you must navigate to the <RM Install Dir>\bin directory.
-location	Oracle database instance name (connection stream).
-project	Name of the instance to be backed up.
-password	Password that is used for the instance, <i>not</i> the Dimensions RM user account password.
-buffer (optional)	<b>Valid values: 1...100</b> Size of the buffer, as a positive integer. This is the amount of temporary space needed to complete the Oracle import/export command. For example, -buffer 65 reserves 65 MB of buffer space. The buffer size can be a maximum of 100 MB, and the default is 50 MB.
-dumpfile	Name and location of the backup file. When it is created, the name is appended with a <DateTimeStamp> and a .dmp extension. The timestamp format is DD_MM_YYYY_HH_MI_SS. In Legacy Mode, if no path is specified, the file is stored in the Saved Projects folder of the <RM Install Dir> directory. In non-legacy mode, the location is relative to the Oracle directory path on the server.
-legacy	<b>Valid values: yes, no</b> <b>Yes</b> creates a backup file using the legacy format. <b>No</b> uses the newer format.  <b>NOTE</b> When running in Amazon Cloud mode, backups can only be created in legacy mode. For further information, see chapter " <a href="#">Using RM Manage within the Amazon Cloud</a> " on page 262.
-rmdbausername	<b>Valid value: ICDBA</b> The Oracle user ID for icmanage.
-rmdbapassword	The password of the Oracle user ID for icmanage.
-encrypt	<b>Valid values: yes, no</b> Specify <b>Yes</b> when using encrypted passwords. Specify <b>No</b> or do not use the -encrypt option when using passwords which are not encrypted.

## Backing up in Normal Mode under Oracle



**NOTE** When running in Amazon Cloud mode, backups can only be created in legacy mode. For further information, see chapter ["Using RM Manage within the Amazon Cloud"](#) on page 262.

To create your backup in **Normal Mode**, use the following syntax (all in one line):

```
icmanage -location <DatabaseInstanceName>
-project <InstanceName>
-password <InstancePassword>
[-buffer <BufferSize>]
-dumpfile <PathAndNameOfBackupFileToCreate>
-legacy no
-rmdbausername ICDBA
-rmdba_password <ICDBAPassword>
```

### Example

The following command backs up an RM instance with a password of `pwd` to a file named `rminstancebackup` in the backup directory of the E drive. The Oracle instance name is `orcl1`.

```
icmanage -location orcl1 -project rminstance -password pwd -dumpfile
e:\backup\rminstancebackup -legacy no -rmbausername ICDBA
-rmbapassword ICDBA
```

When you execute this command, the backup file `rminstancebackup<timestamp>.dmp` is created in the backup folder on drive E. If the backup folder does not exist, it is also created. The buffer size is the default of 50 MB.

### Backing up with Encrypted Passwords in Normal Mode

```
icmanage -location <DatabaseInstanceName>
-project <InstanceName>
-password <encrypted_InstancePassword>
[-buffer <BufferSize>]
-dumpfile <PathAndNameOfBackupFileToCreate>
-legacy no
-rmdbausername ICDBA
-rmbapassword <encrypted_ICDBAPassword>
-encrypt yes
```

To learn how to get encrypted passwords, see chapter ["Backing up with Encrypted Password"](#) on page 199.

### Example

The following command backs up an RM instance with encrypted passwords to a file named `rminstancebackup` in the backup directory of the E drive. The Oracle instance name is `orcl1`.

```
icmanage -location orcl1 -project rminstance -password 8548FE01CD673210
-dumpfile e:\backup\rminstancebackup -legacy no -rmbausername ICDBA
-rmbapassword 9674BA5269718A05 -encrypt yes
```

When you execute this command, the backup file `rinstancebackup<timestamp>.dmp` is created in the backup folder on drive E. If the backup folder does not exist, it is also created. The buffer size is the default of 50 MB.

### **Backing up in Legacy Mode under Oracle**

If the Oracle database is installed in Amazon's AWS cloud, backups must be created in Legacy mode. For other environments it is recommended to use the Normal Mode (see chapter "[Backing up in Normal Mode under Oracle](#)" on page 197).

To create your backup in **Legacy Mode**, use the following syntax (all in one line):

```
icmanage -location <DatabaseInstanceName>
-project <InstanceName>
-password <InstancePassword>
[-buffer <BufferSize>]
-dumpfile <PathAndNameOfBackupFileToCreate>
-rmdbausername ICDBA
-rmdbapassword <ICDBAPassword>
-legacy yes
```

#### **Example**

The following command backs up an RM instance with a password of `pwd` to a file named `rinstancebackup` in the backup directory of the E drive. The Oracle instance name is `orcl1`.

```
icmanage -location orcl1 -project rinstance -password pwd -dumpfile
e:\backup\rinstancebackup -legacy yes -rmbausername ICDBA
-rmbapassword ICDBA
```

When you execute this command, the backup file `rinstancebackup<timestamp>.dmp` is created in the backup folder on drive E. If the backup folder does not exist, it is also created. The buffer size is the default of 50 MB.

### **Backing up with Encrypted Passwords in Legacy Mode**

```
icmanage -location <DatabaseInstanceName>
-project <InstanceName>
-password <encrypted_InstancePassword>
[-buffer <BufferSize>]
-dumpfile <PathAndNameOfBackupFileToCreate>
-legacy yes
-rmdbausername ICDBA
-rmdbapassword <encrypted_ICDBAPassword>
-encrypt yes
```

To learn how to get encrypted passwords, see chapter "[Backing up with Encrypted Password](#)" on page 199.

#### **Example**

The following command backs up an RM instance with encrypted passwords to a file named `rinstancebackup` in the backup directory of the E drive. The Oracle instance name is `orcl1`.

```
icmanage -location orcl1 -project rinstance -password 8548FE01CD673210
-dumpfile e:\backup\rinstancebackup -legacy yes -rmbausername ICDBA
-rmbapassword 9674BA5269718A05 -encrypt yes
```

When you execute this command, the backup file `rminstancebackup<timestamp>.dmp` is created in the backup folder on drive E. If the backup folder does not exist, it is also created. The buffer size is the default of 50 MB.

### **Backing up with Encrypted Password**

For both, Normal Mode and Legacy Mode, you can use encrypted passwords. When using encrypted passwords, you have to add `-encrypt yes` to the command line. Note that you have to encrypt both, instance password and RMDBA password.

To get the encrypted password, follow these steps:

- 1 Open a Command Prompt.
- 2 Change directory to `<RM Install Dir>\bin`.
- 3 Type `AlfEventEmitter -l c:\test -p YOUR_PASSWORD`  
(Replace `YOUR_PASSWORD` with the password you want to encrypt.)
- 4 Hit **Enter**.  
The next line in the Command Prompt shows:  
Encrypted value = "YOUR\_ENCRYPTED\_PASSWORD"
- 5 Copy the encrypted password into your `icmanage` command line.

### **Backing up under MS SQL Server**

For MS SQL Server, the backup does always include the full database.

To create your backup, use the following syntax (all in one line):

```
icmanage -location <DatabaseInstanceName>
-dumpfile <PathAndNameOfBackupFileToCreate>
-rmdbapassword <ICDBAPassword>
```

#### **Example**

The following command backs up an RM instance with a password of `pwd` to a file named `rminstancebackup` in the backup directory of the E drive. The SQL Server database instance name is `RTM`.

```
icmanage -location RTM -dumpfile e:\backup\rminstancebackup
-rmdbapassword ICDBA
```

When you execute this command, the backup file `rminstancebackup<timestamp>.bak` is created in the backup folder on drive E. If the backup folder does not exist, it is also created. The buffer size is the default of 50 MB.

### **Backing up with an Encrypted Password**

```
icmanage -location <DatabaseInstanceName>
-dumpfile <PathAndNameOfBackupFileToCreate>
-rmdbapassword <encrypted_ICDBAPassword>
-encrypt yes
```

To learn how to get encrypted passwords, see chapter ["Backing up with Encrypted Password" on page 199](#).

**Example**

The following command backs up an RM instance with encrypted passwords to a file named `rinstancebackup` in the backup directory of the E drive. The SQL Server instance name is `RTM`.

```
icmanage -location RTM -dumpfile e:\backup\rinstancebackup  
-rmdbapassword 9674BA5269718A05 -encrypt yes
```

When you execute this command, the backup file `rinstancebackup<timestamp>.bak` is created in the backup folder on drive E. If the backup folder does not exist, it is also created. The buffer size is the default of 50 MB.

**Backing up under PostgreSQL**

To create your backup, use the following syntax (all in one line):

```
icmanage -location <DatabaseInstanceName>  
-project <InstanceName>  
-password <InstancePassword>  
-dumpfile <PathAndNameOfBackupFileToCreate>  
-rmdbausername ICDBA  
-rmdba_password <ICDBAPassword>
```

**Example**

The following command backs up an RM instance with a password of `pwd` to a file named `rinstancebackup` in the backup directory of the E drive. The PostgreSQL instance name is `DRM`.

```
icmanage -location DRM -project rinstance -password pwd -dumpfile  
e:\backup\rinstancebackup -rmdbausername ICDBA -rmdbapassword ICDBA
```

When you execute this command, the backup file `rinstancebackup<timestamp>.pgdmp` is created in the backup folder on drive E. If the backup folder does not exist, it is also created.

**Backing up with Encrypted Passwords**

```
icmanage -location <DatabaseInstanceName>  
-project <InstanceName>  
-password <encrypted_InstancePassword>  
dumpfile <PathAndNameOfBackupFileToCreate>  
-rmdbausername ICDBA  
-rmdbapassword <encrypted_ICDBAPassword>  
-encrypt yes
```

To learn how to get encrypted passwords, see chapter ["Backing up with Encrypted Password" on page 199](#).

**Example**

The following command backs up an RM instance with encrypted passwords to a file named `rinstancebackup` in the backup directory of the E drive. The PostgreSQL instance name is `DRM`.

```
icmanage -location DRM -project rinstance -password 8548FE01CD673210  
-dumpfile e:\backup\rinstancebackup -rmdbausername ICDBA  
-rmdbapassword 9674BA5269718A05 -encrypt yes
```

When you execute this command, the backup file `rinstancebackup<timestamp>.pgdmp` is created in the backup folder on drive E. If the backup folder does not exist, it is also created.

## Converting Database and Instances

The database and the RM instances must be converted when upgrading Dimensions RM or restoring an instance account that was created with an older version of Dimensions RM.


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

- 1 Right click on the Dimensions RM database in the left-hand graphical tree and select **Convert Database** from the shortcut menu. This opens the **Database Validation** dialog.
- 2 Expand the Dimensions RM database, by clicking the + sign next to its name. This opens the **ICDBA Password** dialog.
- 3 Enter the password for the ICDBA user and click **OK**.  
If the database needs to be upgraded, you will find the database name is suffixed (not current).
- 4 If RM Manage shows a message to update the database, confirm the automatic update request by clicking **Yes**. If you want to update the database manually, select the database name and click **Upgrade**.
- 5 To upgrade an instance, do the following:
  - a Select an instance account that requires updating. Any instance that shows (Current) after its name, **does not** require updating.
  - b Click **Upgrade**. This opens the **Conversion Progress** dialog.
  - c Click **Continue** to start the conversion process.
  - d When the **Conversion Progress** dialog reports that the upgrade has been completed successfully, click **Close**.
  - e Repeat steps a-d for any other instances that require upgrading.
- 6 When all instances have been upgraded, click **Close** to close the **Database Validation** dialog.

## Deleting an Instance Account

When you delete an instance account, the instance user account and all data associated with the account is deleted from Oracle. You cannot retrieve deleted instance data.


### To delete an instance account:

- 1 In **RM Manage**, select the instance you want to delete.
- 2 Select **File | Delete Instance Account**, click the **Delete** button , or right-click the instance and select **Delete Instance Account**.

- 3 Click **Yes** to confirm the deletion.

## Defining the Instance Schema

### To define the instance schema:

- 1 In **RM Manage**, select the instance for which you want to define the schema.
- 2 Select **File | Define Instance Schema**, click the **Define Instance Schema**  button, or right-click and select **Define Instance Schema**. The Class Definition tool appears.
- 3 Define the instance schema in the Class Definition tool. Refer to ["Class Definition" on page 265](#) for information about Class Definition.


## Backing Up an Instance Schema



### NOTE

- Instance schemas can only be backed up if an Oracle database is used.
- You cannot backup an instance schema when running in Amazon Cloud mode. For further information, see chapter ["Using RM Manage within the Amazon Cloud" on page 262](#).

### To back up instance schema:

- 1 In **RM Manage**, select the instance you want to back up.
- 2 Select **File | Backup/Restore Instance Schema**, click the **Backup/Restore Instance Schema** button , or right-click the instance and select **Backup/Restore Instance Schema**. The **Backup/Restore Schema** dialog box opens.

(See also ["Dimensions RM Backup" on page 182](#), which explains the difference between an instance account and an instance schema.)

- 3 Enter the path on the Oracle server under which you want to save the schema.
- 4 Enter the file name under which you want to save the schema.

- 5 By default, the **Include Security Data** option is selected. This will import all user accounts, group assignments and associated permissions defined in the instance schema. If the group and user information is not needed in the new instance, clear the option.
- 6 Click **Backup**. This opens the **Backup instance schema** dialog which shows the output from the backup. This output is saved in a log file in the directory to which you saved the schema. The log file has the same name apart from the addition `_Exp` and the file extension, which is `.log` instead of a `.cdd`.
- 7 Click **Close** to close the **Backup instance schema** dialog.
- 8 Click **Close** to close the **Backup/Restore Instance Schema** dialog.


## Restoring an Instance Schema from a Backup



### NOTE

- Instance schemas can only be restored up if an Oracle database is used.
- You cannot restore an instance schema when running in Amazon Cloud mode. For further information, see chapter ["Using RM Manage within the Amazon Cloud"](#) on page 262.

### To restore an instance schema from backup:

- 1 In **RM Manage**, select the instance you want to restore.
- 2 Select **File | Backup/Restore Instance Schema**, click the **Backup/Restore Instance Schema** button , or right-click the instance and select **Backup/Restore Instance Schema**. The **Backup/Restore Schema** dialog box opens.

(See also ["Restoring an Instance Account from a Backup"](#) on page 189, which explains the difference between an instance account and an instance schema.)

- 3 Enter the path on the Oracle server under which you want to save the schema.
- 4 Enter the file name under you wish to restore the schema from.


- 5 By default, the **Include Security Data** option is selected. This will import all user accounts, group assignments and associated permissions defined in the instance schema. If the group and user information is not needed in the new instance, clear the option.
- 6 Click **Restore**.
- 7 Into the **From User** box and **Tablespace** box, enter the instance name from which this schema was exported. Then, click **OK**. This opens the **Restore instance schema** dialog which shows the output from the backup. This output is saved in a log file in the directory to which you saved the schema. The log file has the same name apart from the addition `_Imp` with a time stamp, and the file extension, which is `.log` instead of a `.cdd`.

The existing tablespace may not be large enough to accommodate the data contained in the instance that is being restored. In this case, you will be asked if you would like to resize the tablespace prior to continuing. See ["Resizing a Tablespace" on page 239](#) for information about resizing the tablespace.
- 8 Click **Close** to close the **Restore instance schema** dialog.
- 9 Click **Close** to close the **Backup/Restore Instance Schema** dialog.

## Placing an Instance Account Online

If you have placed an instance offline to perform backups or to prevent users from accessing an instance, you can place it online again.


### To place an instance account online:

- 1 In **RM Manage**, select the instance you want to place online.
- 2 Select **File | Place Instance Account Online**, click the **Place Instance Account Online**  button, or right-click and select **Place Instance Account Online**.

## Placing an Instance Account Offline


Placing an instance offline is a convenient way to stop users from accessing an instance. You can also place an instance offline when performing backups.

### To place an instance account offline:

- 1 In **RM Manage**, select the instance you want to place offline.
- 2 Select **File | Place Instance Account Offline**, click the **Place Instance Offline**  button, or right-click and select **Place Instance Account Offline**.


## Installing Instance Tables

### To install instance tables:

- 1 In **RM Manage**, select the instance for which you want to install tables.
- 2 Select **File | Install Instance Tables**, click the **Install Instance Tables** button , or right-click the instance and select **Install Instance Tables**.
- 3 Click **Yes** to confirm the installation.

## Dropping Instance Tables


### To drop instance tables:

- 1 In **RM Manage**, select the instance for which you want to drop tables.
- 2 Select **File | Drop Instance Tables**, click the **Drop Instance Tables** button , or right-click the instance and select **Drop Instance Tables**.
- 3 Click **Yes** to confirm the deletion.

## Recreating Database Procedures

Use this function to ensure that you are using the most recent database procedures. For example, you may want to recreate database procedures after a compilation failure. Recreating the database procedures will synchronize them with the installed version of Dimensions RM.


### To recreate database procedures:

- 1 In **RM Manage**, select the instance for which you want to recreate the database procedures.
- 2 Select **File | Recreate Procedures**, click the **Recreate Database Procedures** button , or right-click the instance and select **Recreate Database Procedures**.
- 3 Click **Yes** to confirm the recreation.

## Recreating Database Indexes

Recreating database indexes increases Dimensions RM performance. This function rebuilds the database trees of Dimensions RM, which may become fragmented during use.


### To recreate database indexes:

- 1 In **RM Manage**, select the instance for which you want to recreate the database indexes.
- 2 Select **File | Recreate Indexes**, click the **Recreate Database Indexes** button , or right-click the instance and select **Recreate Database Indexes**.
- 3 Click **Yes** to confirm the recreation.

## Recreating Database Resources

You can recreate database resources if the database becomes damaged. This function verifies that a unique ID is assigned to the database resources.

### To recreate database resources:

- 1 In **RM Manage**, select the instance for which you want to recreate the database resources.
- 2 Select **File | Recreate Resources**, click the **Recreate Resources** button , or right-click the instance and select **Recreate Resources**.
- 3 Click **Yes** to confirm the recreation.


## Setting Link Options for Baselines

By default, users cannot modify (create or delete) links between objects that are in the *same* baseline. However, you can enable this ability on a baseline by baseline basis in RM Manage.



**NOTE** Users can always modify links if the objects are in different baselines or if only one of the objects is in a baseline. The setting described here does not affect that ability.

### To set link options for baselines:

- 1 In **RM Manage**, select the instance containing the baselines you want to modify.
- 2 Click the **Baseline Link(s)**  button. The **Baseline link(s)** dialog box opens. All baselines in the current instance appear.
- 3 To allow users to modify links in a baseline, deselect the baseline. To prevent users from modifying links in a baseline, select the baseline.
- 4 Click **OK**.

## Managing Users and Groups



**NOTE** The ability to define and manage User and Group Information can now be done in the RM Browser, please see the sections **Managing Users** and **Managing Groups** in the "RM Browser User's Guide."

This functionality is still available in RM Manage, but will be removed in an upcoming release.

In the Dimensions RM environment, an instance represents a work area within which information is created and maintained. Only instances that the current user is allowed to administer will be available.

### Administering Users

Dimensions RM users are maintained for each database and the users are shared across all instances contained within that database. Dimensions RM users are used to maintain security with the Dimensions RM tools.

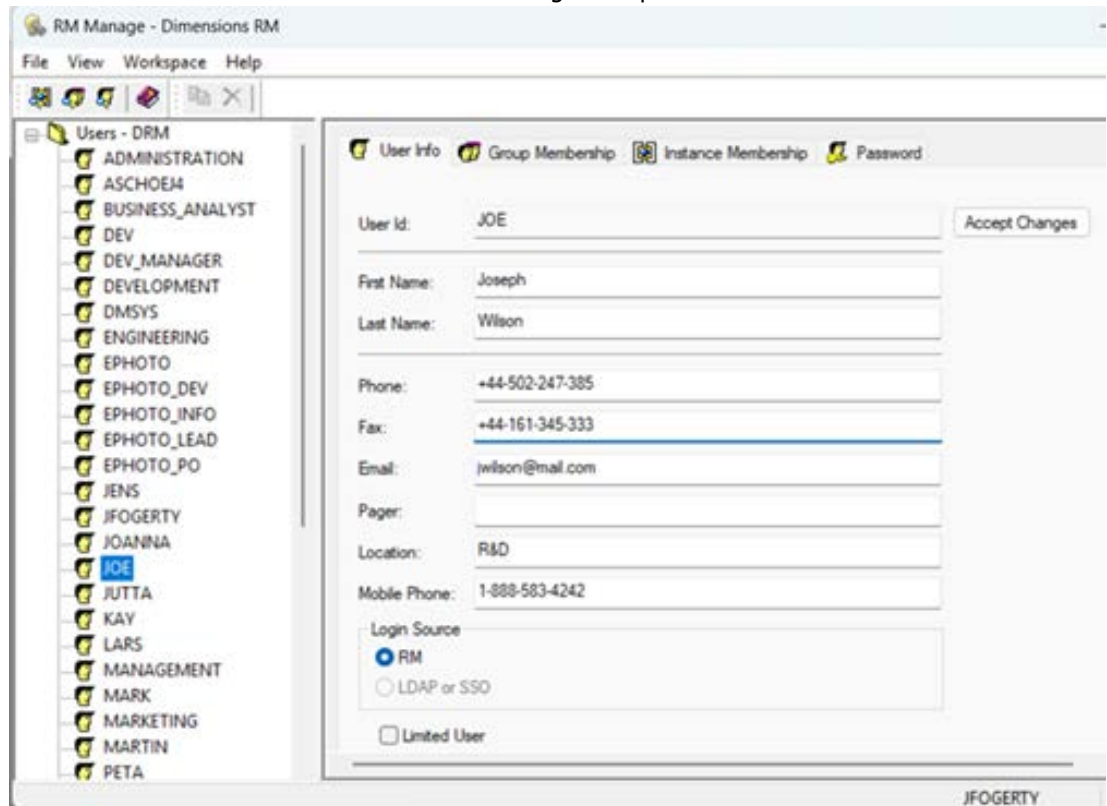
In order to administer users, at least one Dimensions RM instance must exist in the database and an instance administrator must have logged onto the database. Only instance administrators and instance admins are allowed to modify user information.

#### **Creating a New User**

##### To create a new user:

- 1 In **RM Manage**, select **View | Users**.
- 2 Select the "Users - <Dimensions\_RM\_active\_database\_name>" folder at the top of the left-hand graphical tree (for example, **Users - RM**).

- 3 Select **File | New User**, click the **New User**  button, or right-click and select **New User**.
- 4 Type the name of the new user.
- 5 Press **Enter**. The user information dialog box opens.



- 6 On the **User Info** tab, do the following:
  - a Type the general user information.
  - b When using LDAP or SSO for login, select the **Login Source**.
  - c Click **Accept Changes**.
- 7 When using **RM** as **Login Source**, do the following:
  - a Select the **Password** tab.
  - b Enter a password in the **Password** field.
  - c Enter the password again in the **Confirm Password** field.
  - d Select one or more of the following password options:
    - **User Must Change Password at Next Logon**
    - **User Cannot Change Password**
    - **Password Never Expires**

■ **Account Disabled**



**NOTE** If you do not select a password option, users must change their passwords every 60 days. Users get a warning that gives them the opportunity to change their password 14 days before their current password is due to expire. The warning is displayed every time users log in using any Dimensions RM tool.

e Click **Accept Changes**.




**NOTE** For information about password security, see "[Setting Up Password Security](#)" on page 258.

- 8 When using **LDAP or SSO** as **Login Source** and you want to disable the account, do the following:
  - a Select the **Password** tab.
  - b Select **Account Disabled**.
  - c Click **Accept Changes**.

### ***Copying a User***

#### **To copy an existing user:**

- 1 In **RM Manage**, select **View | Users**.
- 2 Select the user you want to copy from the "**Users - <Dimensions\_RM\_active\_database\_name>**" folder at the top of the left-hand graphical tree (for example, **Users - RM**).
- 3 Select **File | Copy User**, click the **Copy User**  button, or right-click and select **Copy User**.
- 4 Type the name of the new user.

- 5 Press **Enter**. The user information dialog box opens.

The screenshot shows the 'RM Manage - Dimensions RM' application window. On the left is a tree view of users under 'Users - DRM', with 'JOE' selected. The main area displays the 'User Info' tab for user 'JOE'. The fields are as follows:

User Id:	JOE	Accept Changes
First Name:	Joseph	
Last Name:	Wilson	
Phone:	+44-502-247-385	
Fax:	+44-161-345-333	
Email:	jwilson@mail.com	
Pager:		
Location:	R&D	
Mobile Phone:	1-888-583-4242	
Login Source:	<input checked="" type="radio"/> RM <input type="radio"/> LDAP or SSO	
	<input type="checkbox"/> Limited User	

- 6 On the **User Info** tab, do the following:
- Type the general user information.
  - Select the **Login Source**.
  - Click **Accept Changes**.
- 7 When using **RM** as **Login Source**, do the following:
- Select the **Password** tab.
  - Enter a password in the **Password** field.
  - Enter the password again in the **Confirm Password** field.
  - Select one or more of the following password options:
    - **User Must Change Password at Next Logon**
    - **User Cannot Change Password**
    - **Password Never Expires**
    - **Account Disabled**



**NOTE** If you do not select a password option, users must change their passwords every 60 days. Users get a warning that gives them the opportunity to change their password 14 days before their current password is due to expire. The warning is displayed every time users log in using any Dimensions RM tool.

- e Click **Accept Changes**.



**NOTE**


- Copying a user copies permissions (e.g. the "Create Class" right), assigned groups, instance assignments and the user info.
- For information about password security, see ["Setting Up Password Security" on page 258](#).

- 8 When using **LDAP or SSO** as **Login Source** and you want to disable the account, do the following:
  - a Select the **Password** tab.
  - b Select **Account Disabled**.
  - c Click **Accept Changes**.

***Deleting a User***

**To delete a user:**

- 1 In **RM Manage**, select **View | Users**.
- 2 Select the user in the left-hand graphical tree that you want to delete.

Only users that have not been assigned to any instances should be deleted. If the user profile is deleted it will be removed from every instance that it has been assigned to.
- 3 Select **File | Delete User**, click the **Delete User**  button, or right-click and select **Delete User**.
- 4 Click **Yes** to confirm the deletion.

***Changing User General Information***

**To change general information for a user:**

- 1 In **RM Manage**, select **View | Users**.
- 2 Select the user in the left-hand graphical tree for which you want to change the general information.
- 3 Click the **User Info** tab.
- 4 Enter new user information.
- 5 Click **Accept Changes**.


***Updating User General Information for All Users***

You can update the general information for all users with the data specified on your LDAP server. To allow this, you must have set up RM to use LDAP. The following criteria have to be met:

- The LDAP server must have been specified (see chapter ["Specifying an LDAP Server" on page 252](#)).

- A valid LDAP configuration must have been specified (see chapter "[Specifying the LDAP Configuration](#)" on page 252).
- LDAP must have been specified as a login source (see chapter "[Specifying Login Sources in RM Manage](#)" on page 247).
- LDAP attributes must match your LDAP environment (see section "[Configuring LDAP Attributes to match the environment](#)" on page 211).

**To update the general information for all users, execute these steps:**

- 1 In **RM Manage**, select **View | Users**.
- 2 In the users list, select the folder on top (labeled **Users - Database Name**).
- 3 Click  .
- 4 Confirm the following dialog by clicking **Yes**.

**Configuring LDAP Attributes to match the environment**

To allow RM using LDAP data, it is essential that RM knows the attributes used by your LDAP server. If your LDAP server uses the default LDAP setup, there is no need to configure the LDAP attributes. The following table shows the names of the RM attributes, the registry value for configuration and the default LDAP attribute names.

RM Attribute	Registry Value	Default LDAP Attribute
First Name	LDAP_ATTR_FIRST_NAME	givenName
Last Name	LDAP_ATTR_LAST_NAME	sn
Phone	LDAP_ATTR_PHONE	telephoneNumber
Fax	LDAP_ATTR_FAX	otherFacsimileTelephoneNumber
Email	LDAP_ATTR_EMAIL	mail
Pager	LDAP_ATTR_PAGER	pager
Location	LDAP_ATTR_LOCATION	location
Mobile Phone	LDAP_ATTR_MOBILE_PHONE	mobile

**To configure the LDAP mapping, execute these steps:**

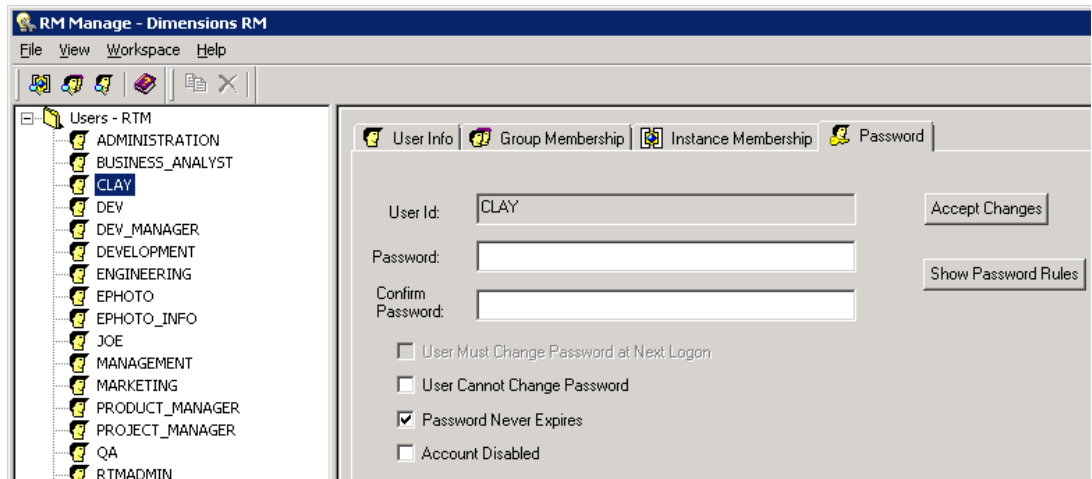
- 1 Open Windows Registry editor (select **Run**, enter `regedit` and click **OK**).
- 2 Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Micro Focus\Dimensions RM\Environment\Default`.
- 3 Right-click the **Default** key and select **New | String Value** from the shortcut menu.
- 4 Specify the LDAP registry value (e.g. `LDAP_ATTR_FIRST_NAME`) and press **Enter**.
- 5 Double-click the value you just created. This opens the **Edit String** dialog.
- 6 Enter the name of the LDAP attribute into the **Value data** box.

- 7 Click **OK**.
- 8 Repeat steps 3 - 7 for any other LDAP attributes you want to configure.
- 9 If RM Manage is running, close it and start it again.

### **Changing User Password Information**

#### **To change user password information:**

- 1 In **RM Manage**, select **View | Users**.
- 2 Select the user in the left-hand graphical tree for which you want to change the password information.
- 3 Click the **Password** tab.



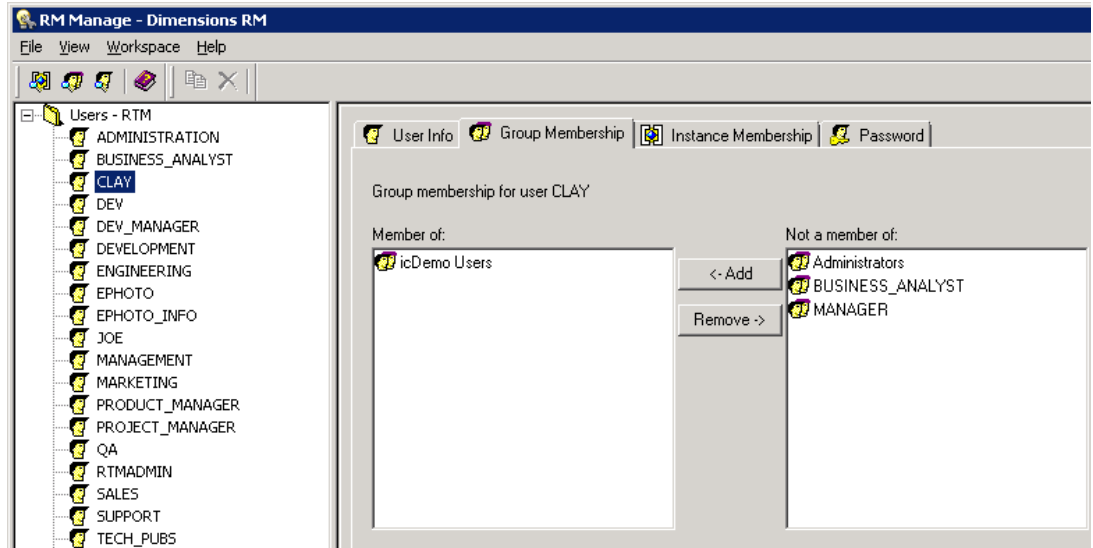
- 4 Enter new user password information.
- 5 Click **Accept Changes**.

### **Adding a User to a Group**

#### **To add a user from the user view:**

- 1 In **RM Manage**, select **View | Users**.
- 2 Select the user in the left-hand graphical tree you want to add to a group.

- 3 Click the **Group Membership** tab.



- 4 Select the groups to which you want to add the user from the list on the right.

- 5 Click **Add**.

#### To add a user from the group view:

- 1 In **RM Manage**, select **View | Groups**.
- 2 Select the group in the left-hand graphical tree to which you want to add a user.
- 3 Click the **Members** tab.
- 4 Select the users that you would like to add to the group from the list on the right.
- 5 Click **Add**.

#### *Removing a User from a Group*

##### To remove a user from the user view:

- 1 In **RM Manage**, select **View | Users**.
- 2 Select the user in the left-hand graphical tree you want to remove from a group.
- 3 Click the **Group Membership** tab.
- 4 Select the groups from which you want to remove the user from the list on the left.
- 5 Click **Remove**.

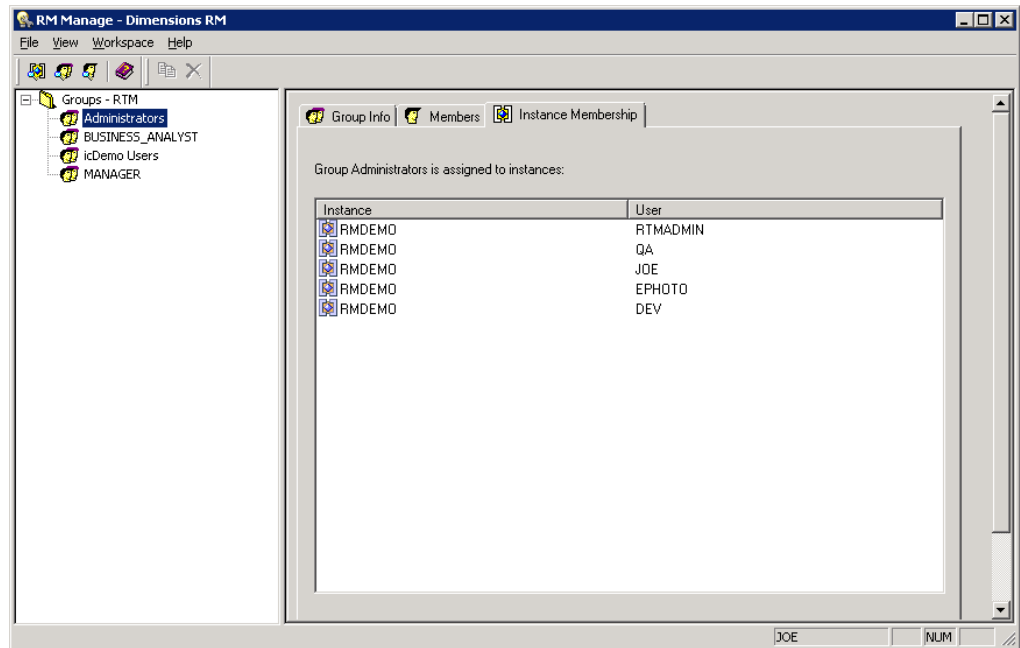
##### To remove a user from the group view:

- 1 In **RM Manage**, select **View | Groups**.
- 2 Select the group in the left-hand graphical tree to which you want to remove a user.
- 3 Click the **Members** tab.
- 4 Select the users that you would like to remove from the group from the list on the left.
- 5 Click **Remove**.

## Viewing Instance Assignment

To view instance assignment:

- 1 In **RM Manage**, do one of the following in the left-hand graphical tree:
  - select **View | Users**, or
  - select **View | Groups**.
- 2 Select the user or group for which you want to view instance assignment.
- 3 Click the **Instance Membership** tab.



## Administering Groups

**NOTE** The ability to define and manage User and Group Information can now be done in the RM Browser, please see the sections *Managing Users* and *Managing Groups* in the "RM Browser User's Guide."

**This functionality is still available in RM Manage, but will be deprecated in an upcoming release.**


Dimensions RM groups are maintained for each database. The groups are shared across all instances contained within that database. Dimensions RM groups are used to maintain security within the Dimensions RM tools.

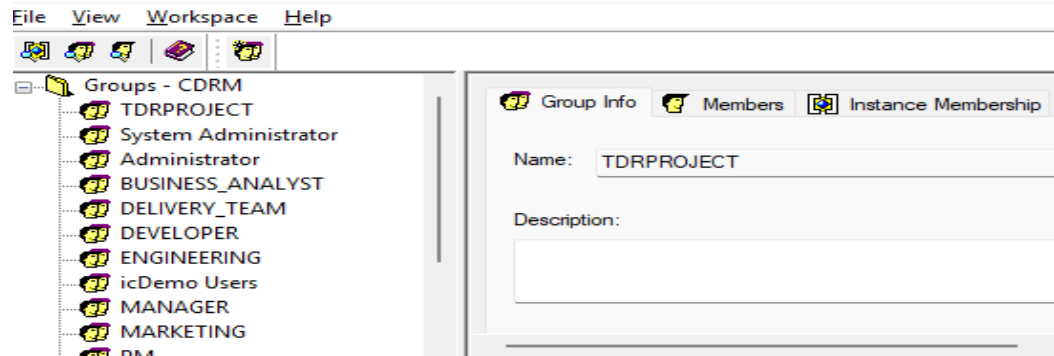
In order to administer groups, at least one Dimensions RM instance must exist in the database and an instance administrator must have logged onto the database. Only instance administrators and instance admins are allowed to modify group information.

### Creating a New Group

To create a new group:

- 1 In **RM Manage**, select **View | Groups**.


- 2 Select the "Groups - <Dimensions\_RM\_active\_database\_name>" folder at the top of the left-hand graphical tree (for example, **Groups - CDRM**).
- 3 Select **File | New Group**, click the **New Group**  button, or right-click and select **New Group**.
- 4 Type the name of the new group and press **Enter**. The group information dialog box opens.

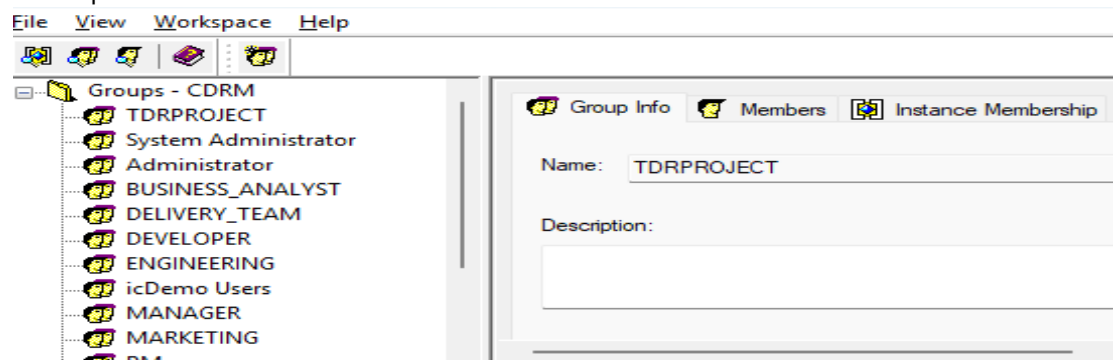


- 5 Click the **Group Info** tab and enter a description for the group.
- 6 Click **Accept Changes**.

### Copying a Group

#### To copy an existing group:

- 1 In **RM Manage**, select **View | Groups**.
- 2 Select the group you wish to copy from the "Groups - <Dimensions\_RM\_active\_database\_name>" folder at the top of the left-hand graphical tree (for example, **Groups - CDRM**).
- 3 Select **File | Copy Group**, click the **Copy Group**  button, or right-click and select **Copy Group**.
- 4 Type the name of the new group and press **Enter**. The group information dialog box opens.



- 5 Click the **Group Info** tab and enter a user description.
- 6 Click **Accept Changes**.

## ***Deleting a Group***

### **To delete a group:**

- 1 In **RM Manage**, select **View | Groups**.
- 2 Select the group in the left-hand graphical tree that you want to delete.



**NOTE** Do not delete a group if a member of that group is assigned to an instance. If such a group is deleted, all members of the group will be removed from every instance to which they are assigned.

- 3 Select **File | Delete Group**, click the **Delete Group**  button, or right-click and select **Delete Group**.



**NOTE** This action cannot be undone.

- 4 Click **Yes** to confirm the deletion.

## ***Changing Group General Information***

### **To change general information for a group:**

- 1 In **RM Manage**, select **View | Groups**.
- 2 Select the group in the left-hand graphical tree for which you want to change the general information.
- 3 Click the **Group Info** tab.
- 4 Enter new group information.
- 5 Click **Accept Changes**.

## **Assigning Users to Groups**

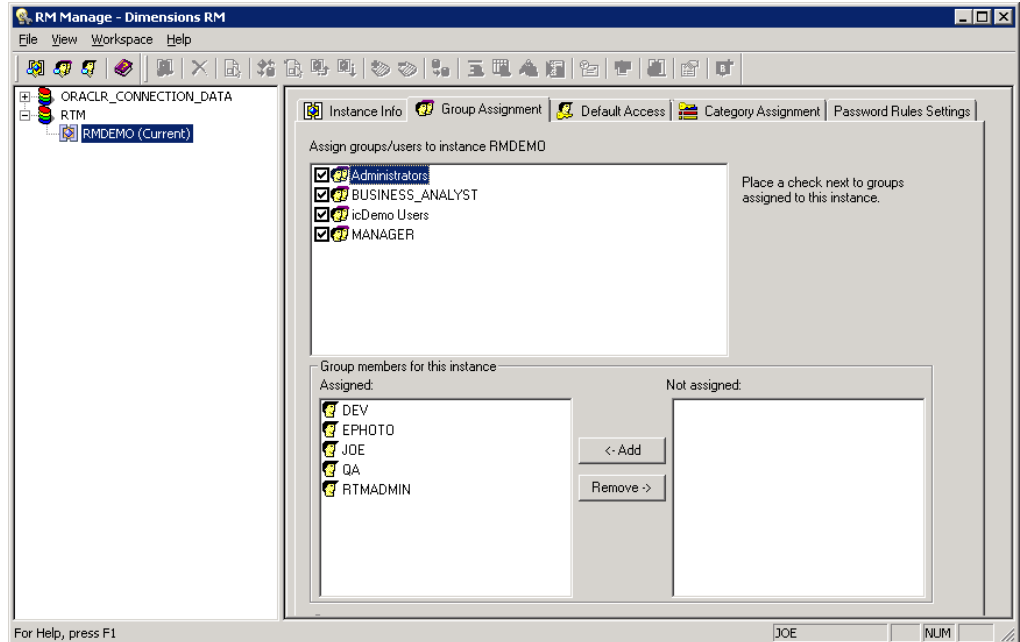
A user must be assigned to an instance through group membership before being allowed access to the instance.

### ***Adding a User to an Instance***

#### **To add a user to an instance:**

- 1 In **RM Manage**, select **View | Instances**.
- 2 Select the instance in the left-hand graphical tree to which you want to add the user.

### 3 Click the **Group Assignment** tab.



- 4 Select the group that contains the user you want to add to the instance. Selecting the check box automatically adds all members of that group to the instance. Clearing the check box automatically removes all members of that group from the instance.
- 5 Select the users from the **Not Assigned** list.
- 6 Click **Add**.

### ***Adding an Administrator to an Instance***

#### **To add an administrator to an instance:**

- 1 Add the user to the Administrators group (see ["Adding a User to a Group"](#) on page 212).
- 2 In **RM Manage**, select **View | Instances**.
- 3 Select the instance in the left-hand graphical tree to which you want to add the administrator user.
- 4 Click the **Group Assignment** tab.
- 5 Select the **Administrators** group.
- 6 Select the user from the **Not Assigned** list.
- 7 Click **Add**.

### ***Removing a User from an Instance***

#### **To remove a user from an instance:**

- 1 In **RM Manage**, select **View | Instances**.

- 2 Select the instance in the left-hand graphical tree from which you want to remove the user.
- 3 Click the **Group Assignment** tab.
- 4 Select the group that contains the user you want to remove from the instance. Selecting the check box automatically adds all members of that group to the instance. Clearing the check box automatically removes all members of that group from the instance.
- 5 Select the users from the **Assigned** list.
- 6 Click **Remove**.

## Group Security

### Resource Types

Groups are granted access rights to Actions within a specific Resource Type (e.g., Class, Documents, Reports, Collections, etc.) or to all Actions within each resource type. For example, Document Actions include Create, Create Based on a Existing Document, Create Snapshot or Delete among others; all or a subset of these Actions may be granted to a group.

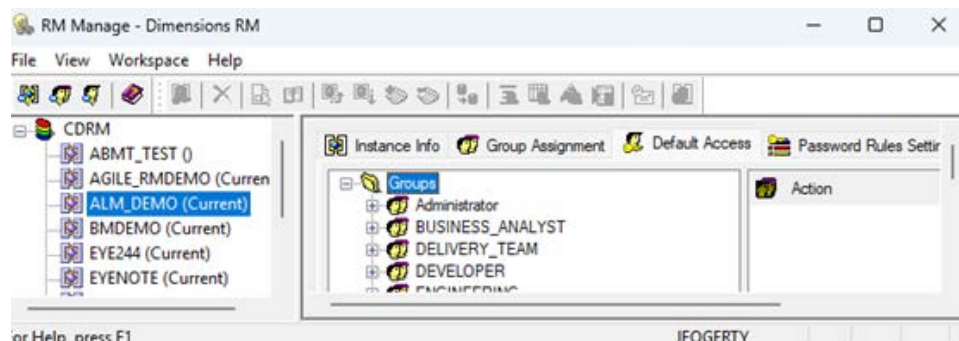
### Showing or Hiding User Permissions - This Feature has been Deprecated

In Dimensions RM Releases prior to Dimensions RM 25.2 (13), it was possible, using RM Manage or Web Services, to assign permissions at the User Level. **This feature has been deprecated.**

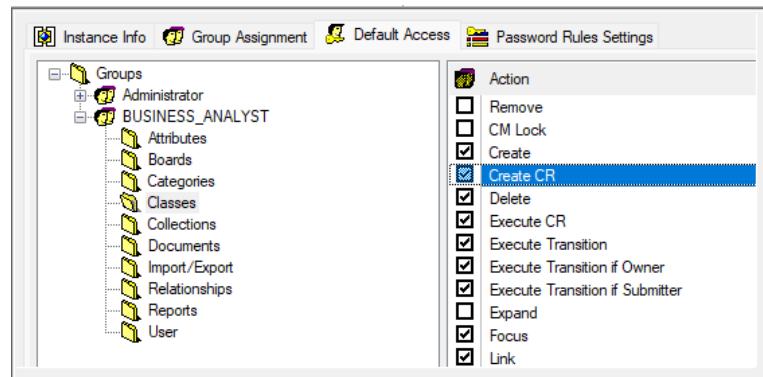
### Setting Default Group Access

Although it remains possible to manage groups from RM Manage, we recommend using Manage Users/Groups in the Dimensions RM Browser for all access management (see Administration > Managing Users, Managing Groups, Managing Teams, and Managing Categories).

- 1 In **RM Manage**, select **View | Instances**.
- 2 Select the instance in the left-hand graphical tree for which you want to set default access.
- 3 Click the **Default Access** tab.



- 4 Click + to expand a **Groups** folder.
- 5 Expand the group to see the types of resources that may be assigned default access.
- 6 Select the type (for example, Classes).



- 7 Click the transaction to toggle the access rights. Select the check box to assign group access rights  or to unassign rights .

### **Setting Default User Access**

In Dimensions RM Releases prior to Dimensions RM 25.2(13), it was possible, using RM Manage or Web Services, to assign permissions at the User Level. **This feature has been deprecated.**

To assign permissions for a single user or for a small subset of users, the Instance Administrator must create a group. Experience has taught us, and our veteran administrators, that maintaining individual user permissions is very difficult.

### **Granting All**

#### **Granting All Access Rights to a Group:**

Groups are granted access rights to Actions within a specific resource type (e.g., Class (requirement types), Documents, Reports, Collections, etc.) or to all Actions within each

resource type. For example, Documents may be Created, Created Based on a Existing Document, Deleted or Removed.



**NOTE Grant All** does not Grant permission to all Actions. There are specific Actions, Remove for example, within several resource types that is not granted by default.

As a good general practice, Open Text recommends that no Dimensions RM group or user (including Administrators) ever be granted the class access rights for: REMOVE, UPDATE, and UPDATE\_NON\_CURRENT.

**Remove** allows the complete removal of an object from the database. The administrator may use this function when hundreds of requirements have been imported in error - otherwise, **Delete** - which marks an object as deleted but leaves it in the database, should be used.

**Update** allows users to modify objects without history control, changes should be performed with the **Save** function which replaces the current object with the changed version; thus maintaining history. For organizations using well-controlled workflow, update permission may be allowed during the draft state - when changes are frequent and change history not critical.

**Update NON\_Current** - changes history. It exists because there have been situations in which organizations have required it - but its use should be avoided.

#### To grant access rights for every Action within a single resource type:

- 1 In **RM Manage**, select **View | Instances**.
- 2 Select the instance in the left-hand graphical tree for which you want to grant default access.
- 3 Click the **Default Access** tab.
- 4 Click + to expand the **Groups** folder.
- 5 Expand the group to see the types of resources that may be assigned default access.
- 6 Right-click the *resource type* to which you want to grant all access rights and select **Grant All**. This sets all of the Actions, except those noted above, in this resource type to be explicitly granted for this group.

#### To grant access rights for every Action in every resource type:

- 1 In **RM Manage**, select **View | Instances**.
- 2 Select the instance in the left-hand graphical tree for which you want to grant default access.
- 3 Click the **Default Access** tab.
- 4 Click + to expand the **Groups** folder.
- 5 Right-click the *group* you want to grant all access rights to and select **Grant All**. This sets all of the transactions in every resource type to be explicitly granted for this group.

## Revoking All

### To revoke access rights for every Actions within a single resource type:

- 1 In **RM Manage**, select **View | Instances**.
- 2 Select the instance in the left-hand graphical tree for which you want to revoke default access.
- 3 Click the **Default Access** tab.
- 4 Click + to expand the **Groups** or **Users** folder.
- 5 Click + next to the relevant group or user to see the types of resources that may be assigned default access.
- 6 Right-click the *resource type* from which you want to revoke all access rights and select **Revoke All**. This sets all of the transactions in this resource type to be denied for this group or user.
- 7 When prompted, click **Yes** to confirm the revoke all action.

### To revoke access rights for every Actions in every resource type:

- 1 In **RM Manage**, select **View | Instances**.
- 2 Select the instance in the left-hand graphical tree for which you want to revoke default access.
- 3 Click the **Default Access** tab.
- 4 Click + to expand the **Groups** or **Users** folder.
- 5 Right-click the *group or user* for which you want to revoke all access rights and select **Revoke All**. This sets all of the transactions in every resource type to be denied for this group or user.
- 6 When prompted, click **Yes** to confirm the revoke all action.

## Assigning Categories




In Dimensions RM you can grant or deny access to requirements, dashboards, documents, reports, collections and baselines for a category. To do this, you can use two different methods:

- [Role Based Category Access](#)
- [User Based Category Assignment](#)

Role based category assignment only allows a per-group assignment. User based category assignment allows to assign rights on categories for groups or users.

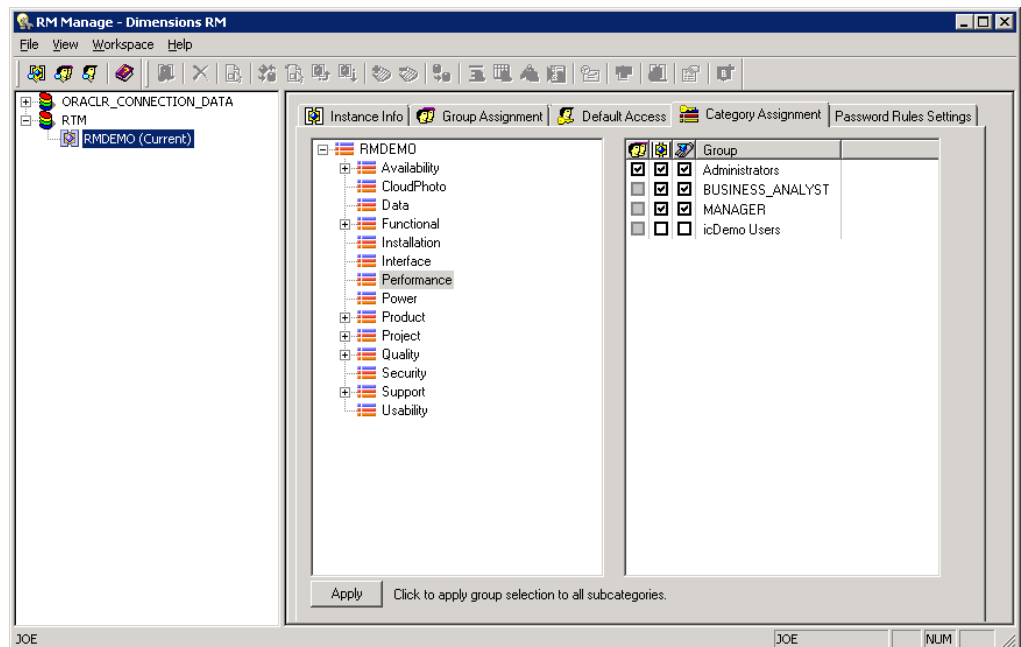
### Role Based Category Access

Permissions are assigned to categories through groups. Only users who are members of groups assigned to a category are able to view this category. The permissions for each category are determined by the permissions the user has from belonging to groups that are assigned to this category. The Administrators group always has permissions to all categories.

- The group column  in the right-hand list allows you to grant group access, deny a group access, or allow a group to inherit the access rights the parent groups.
- The instance column  in the right-hand list shows the access that is provided from the instance level. If this check box is selected, the group is explicitly allowed access to the category at the instance level. It shows whether the group has full access at a global level. You cannot explicitly change this check box selection.
- The actual column  in the right-hand list shows the effective access at the category level. It shows what the group rights are after you change them.

### To assign permissions to categories:

- 1 In **RM Manage**, select **View | Instances**.
- 2 Select the instance in the left-hand graphical tree for which you want to set default access.
- 3 Click the **Category Assignment** tab.



- 4 In the tree in the left pane, select the category to which you want to assign permissions.
- 5 In the right pane, select the check box next to each group you want to assign permissions to this category.
- 6 If you want the group selection to apply to all subcategories, click **Apply** at the bottom of the tab.

### User Based Category Assignment

Permissions are assigned to categories through groups. However, in RM Browser you can define which users are fulfilling this role for a category.



**NOTE** When adding a user to a group, the user has the rights of the group on all categories the group is assigned on.

**Follow these steps to prepare a group for category assignment:**

- 1 Start **RM Manage**.
- 2 Select the database your instance resides in.
- 3 Log in and select the instance.
- 4 Create a group (e.g. *Project\_Manager*) if necessary.
- 5 Assign users to the desired group.
- 6 In Instance View, select the **Default Access** tab.
- 7 Expand the *Project\_Manager* group.
- 8 Select the **Categories** folder.
- 9 Clear the **FullAccess** box.
- 10 Assign other rights as required.

You can now assign users as a role to categories. For further information, see chapter "Assigning Access Rights" in *RM Browser User's Guide*.

**Password Rules Settings Tab**

The use of the **Password Rules Settings** tab is described in "[Setting Password Rules](#)" on [page 259](#).

**Deleting a User from an Instance**

Users cannot be deleted once assigned to an instance through any group. Users must be unassigned from instances before being deleted from the database. Only instance administrators and instance admins can remove users from instances. The administrative user that is generated for an instance cannot be deleted under any circumstances. Dimensions RM maintains this ID internally.

## Managing Security



**NOTE** The ability to define and manage User and Group Information can now be done in the RM Browser, please see the sections **Managing Users** and **Managing Groups** in the "RM Browser User's Guide."

This functionality is still available in RM Manage, but will be removed in an upcoming release.

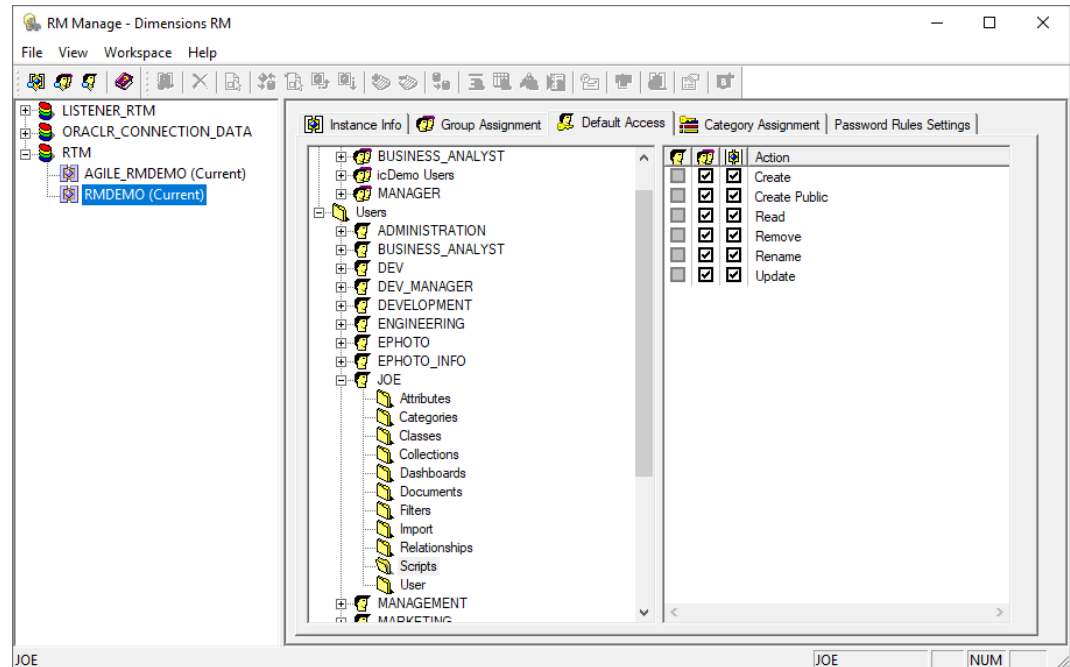
Access rights are associated with each resource defined in a Dimensions RM database. Access rights determine whether a user can perform a particular task on a target resource. (A user refers to an Dimensions RM user, not an Oracle or Windows user.) This section describes the relationships between the various entities that represent users and their permissions and the various means used to manipulate permissions.

## Default Access

Dimensions RM security is maintained by assigning access rights for groups and users. The administrator may assign default access to a group or user, thereby eliminating the need to assign access to each item that is created in the other tools. The default access may be overridden. Refer to "Class Definition" on page 265 and "Order of Precedence" on page 231 for information on overriding default access.

It is through group membership that a user is added to an instance. Once the user has been assigned to an instance, default access may be set for the groups, as well as for the individual user. Each group has two states for default access: granted or not granted. Each user has three states for default access: granted, revoked or inherited. The combination of the user default access as well as the default access for the groups that he or she has been assigned to through the instance determines the default access for that user for the instance.

For example, in the following illustration, the user has been assigned to the instance MYINSTANCE through a group that the user is a member of and has default **Read** and **Create** access granted for the **Scripts** resource type as a user, but does not have this access granted as a default for the associated group.



The user's default access for **Scripts** shows that the **Create** and **Read** transactions are not selected in the group column . Those transactions have not been granted for the groups to which the user belongs. The user column  represents the access that has been set for the user. The rows that are gray  in the user column indicate that the user does not have any default access set for this transaction and will inherit the collective access of group. The rows that are unchecked  indicate that the user has been explicitly denied default access for this transaction. The rows that are checked  indicate that the user has been explicitly granted default access for this transaction.

The instance column  indicates the net effect of the user and group default access for the instance. In this case, the user has **Read** and **Create** access for the resource type of **Scripts**.

---

## Database Administrator Accounts


### Changing Passwords and Unlocking

See also "Changing the Instance Password" on page 181, "Updating the Instance Password" on page 182, and "Changing an Instance Administrator Password" on page 231.

The passwords for Dimensions RM database administrator Oracle accounts ICDBA and ICADMIN can now be changed or unlock from within RM Manage. The unlock function unlocks an account and enables the user.

### *Changing the ICDBA Account Password*

#### To change the ICDBA account password:

- 1 Ensure that RM Manage is running with administrators permissions as you need write access to the security.dat file. If you are not sure if **RM Manage** is running with administrator permissions, do the following:
  - a Exit **RM Manage**.
  - b Right-click the **RM Manage** icon and select **Run as administrator** from the shortcut menu.
  - c Depending on your configuration, you may need to click **Yes** to confirm the **User Access Control** dialog for **RM Manage**.
- 2 In **RM Manage**, select the database whose ICDBA account you want to change the password for.
- 3 Select **File | Change Administrator Password**, click the **Change Administrator Password** button , or right-click the database and select **Change Administrator Password**.
- 4 The **Change administrator password** dialog box opens.

- 5 In the **Select account to modify area** , select the ICDBA from the **Account** list.

- 6 In the **Change account password** area, type the new password for the ICDBA account.



**NOTE** The password is case sensitive.


- 7 In the associated **Confirm Password** field, re-type the password.
- 8 In the **Enter current ICDBA account password** area, type the current ICDBA password into the **Password** box.
- 9 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 to change the ICDBA password before 180 days elapse using the RM Manage **Change Administrator Password** menu item, see "[Database Administrator Accounts](#)" on page 225.

### ***Unlocking the ICDBA Account***

#### **To unlock the ICDBA account:**

- 1 In **RM Manage**, select the database whose ICDBA account you want to unlock.
- 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 account from the **Account** list.

The screenshot shows a dialog box titled "Change administrator password". It contains three sections:

- Select account to modify:** A dropdown menu with "ICDBA" selected.
- Change account password:** A section with a checked checkbox labeled "Unlock account". Below it, the "Password" and "Confirm Password" fields are disabled (grayed out).
- Enter SYSDBA account password:** A section with "Account Name" set to "sys" and an empty "Password" field.

At the bottom of the dialog are two buttons: "Unlock" and "Cancel".


- 5 Check the **Unlock account** check box. This will disable the **Password** and **Confirm Password** fields in the **Change account password** area.
- 6 In the **Enter SYSDBA account password** area, specify the user name of a database administrator (for Oracle: sys; for MS SQL Server: sa) and the associated password.
- 7 Click **Unlock**.

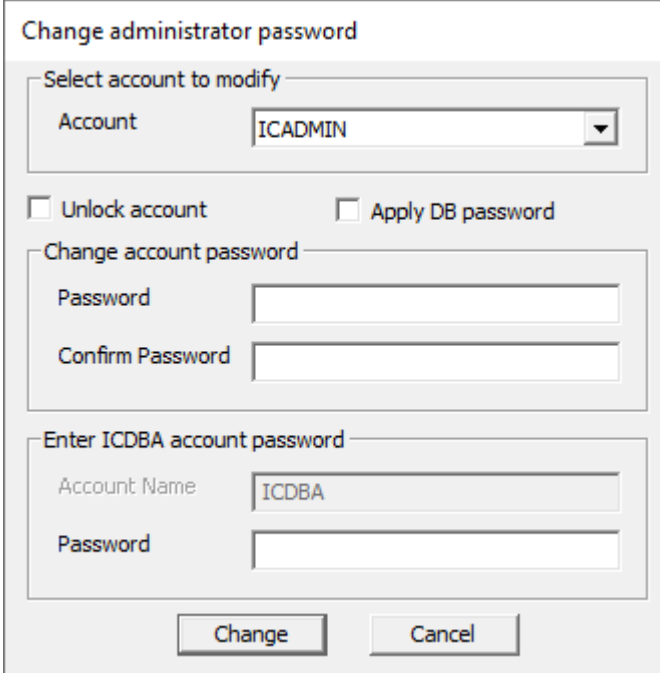
### **Changing the ICADMIN Account Password**

If the password of the ICADMIN account was changed in the database and not through RM Manage, please refer to chapter ["Updating the ICADMIN Password in Security.dat"](#) on page 228.

#### **To change the ICADMIN account password:**

- 1 Ensure that **RM Manage** is running with administrators permissions as you need write access to the security.dat file. If you are not sure if **RM Manage** is running with administrator permissions, do the following:
  - a Exit **RM Manage**.
  - b Right-click the **RM Manage** icon and select **Run as administrator** from the shortcut menu.
  - c Depending on your configuration, you may need to click **Yes** to confirm the **User Access Control** dialog for **RM Manage**.
- 2 In **RM Manage**, select the database whose ICADMIN account you want to change the password for.

- 3 Select **File | Change Administrator Password**, click the **Change Administrator Password** button , or right-click the database and select **Change Administrator Password**.
- 4 The **Change administrator password** dialog box opens.
- 5 In the **Select account to modify area**, select the ICADMIN account the **Account** list.



- 6 In the **Change account password** area, type the new password for the ICADMIN account.



**NOTE** The password is case sensitive.

- 7 In the associated **Confirm Password** field, re-type the password.
- 8 In the **Enter ICDBA account password** area, type the current ICDBA password.
- 9 Click **Change**.




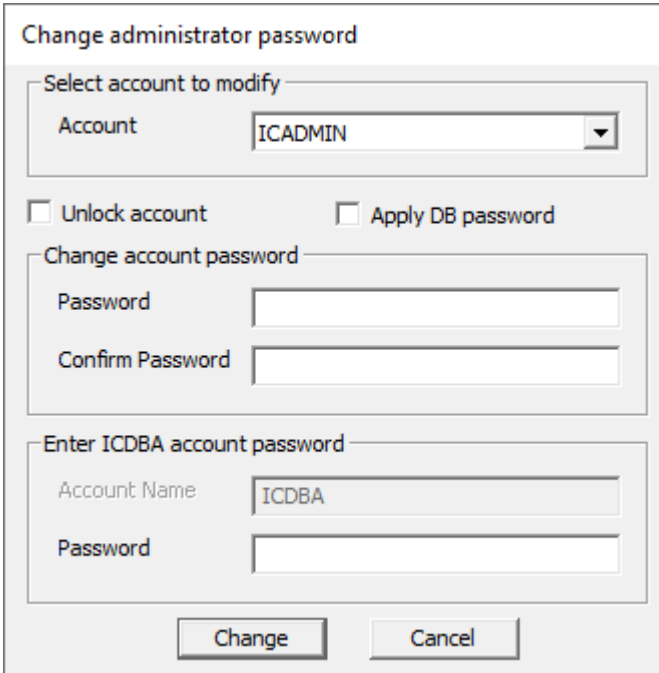
**IMPORTANT!** For the Oracle RDBMS, Oracle account passwords expire by default after 180 days. Unless your DBA has re-configured such RDBMS to override this default and allow permanent passwords, you must to change the ICDBA password before 180 days elapse using the RM Manage **Change Administrator Password** menu item, see ["Database Administrator Accounts" on page 225](#).

### **Updating the ICADMIN Password in Security.dat**

This section covers to update the ICADMIN password in `security.dat`, which can become necessary if the ICADMIN password was changed directly in the database. In this case, the password in the `security.dat` file must be updated to allow Dimensions RM to run. For changing the password of the ICADMIN account also in the database, see chapter ["Changing the ICADMIN Account Password" on page 227](#).

**To update the ICADMIN account password in security.dat:**

- 1 Ensure that RM Manage is running with administrators permissions as you need write access to the security.dat file. If you are not sure if RM Manage is running with administrator permissions, do the following:
  - a Exit **RM Manage**.
  - b Right-click the **RM Manage** icon and select **Run as administrator** from the shortcut menu.
  - c Depending on your configuration, you may need to click **Yes** to confirm the **User Access Control** dialog for **RM Manage**.
- 2 In **RM Manage**, select the database whose ICADMIN account password you want to update in the security.dat file.
- 3 Select **File | Change Administrator Password**, click the **Change Administrator Password** button , or right-click the database and select **Change Administrator Password**.
- 4 The **Change administrator password** dialog box opens.
- 5 In the **Select account to modify area**, select the ICADMIN account the **Account** list.



- 6 Select the **Apply DB password** option. This disables the **Confirm password** box and the **Enter ICDBA account password** area.
- 7 In the **Change account password** area, type the new password of the ICADMIN account.




**NOTE** The password is case sensitive.

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 to change the ICDBA password before 180 days elapse using the RM Manage **Change Administrator Password** menu item, see "[Database Administrator Accounts](#)" on page 225.

### ***Unlocking the ICADMIN Account***

#### **To unlock the ICADMIN account:**

- 1 In **RM Manage**, select the database whose ICDBA account you want to unlock.
- 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 ICADMIN account from the **Account** list.

The screenshot shows a dialog box titled "Change administrator password". It contains the following elements:


- Select account to modify:** A dropdown menu with "Account" as the label and "ICADMIN" selected.
- Change account password:** A section with two checkboxes: "Unlock account" (checked) and "Apply DB password" (unchecked). Below these are two text input fields labeled "Password" and "Confirm Password", both of which are empty.
- Enter ICDBA account password:** A section with two text input fields: "Account Name" (containing "ICDBA") and "Password" (empty).
- Buttons:** "Unlock" and "Cancel" buttons at the bottom.

- 5 Check the **Unlock account** check box. This will disable the **Password** and **Confirm Password** fields in the **Change account password** area.
- 6 In the **Enter ICDBA account password** area, type the password of the ICDBA user into the **Password** box.
- 7 Click **Unlock**.

## Changing an Instance Administrator Password

See also ["Changing the Instance Password" on page 181](#) and ["Database Administrator Accounts" on page 225](#).

**To change the administrator password for the currently selected instance:**

- 1 In **RM Manage**, select the database (for the current selected instance) for which you want to change the instance administrator password.
- 2 Select **File | Change User Password**, click the **Change User Password** button , or right-click the database and select **Change User Password**. The **Change user password** dialog box opens.
- 3 Enter your system administrator password.
- 4 Click **OK**. This opens the **Change Instance Password/Instance Admin Password** dialog.
- 5 Enter the current password of the instance administrator into the **Current Password for InstanceAdmin** box.
- 6 Enter the new password into the **New Password for InstanceAdmin** box.
- 7 Re-type the new password into the **Confirm New Password for InstanceAdmin** box.
- 8 Select the **Retain the current Instance (DB) password** option. This disables all password options for the instance.
- 9 Click **OK**.

## Order of Precedence

The use of groups and the ability to explicitly allow and disallow users access to a resource make it possible that a user may be both allowed and denied access to a specific resource. To resolve this potential conflict into a simple Boolean condition or access right, an order of precedence is used by Dimensions RM security from highest to lowest precedence:

Source of Access	Allowed Status
An individual user has been explicitly denied access to a resource/transaction.	Denied
An individual has been granted explicit access to a resource/transaction.	Allowed
An individual has been granted access to a resource/transaction through membership in a group, which has been granted access.	Allowed
An individual has been explicitly denied access to an entire resource type through default access rights.	Denied
An individual has been explicitly allowed access to an entire resource type through default access rights.	Allowed

Source of Access	Allowed Status
An individual has been allowed to an entire resource type through membership in a group, which has been granted access rights to a resource type.	Allowed
There exist no entries specifying access rights for the individual or any groups that the individual is a member of in the access rights list.	Denied

**NOTE**

- Even if the administrator denied certain users the **Rename Baseline** transaction, these users can rename a baseline if they created it. In this situation, the permissions that are denied by the administrator are overridden.
- If a user is denied permission to delete a baseline, they cannot delete any baseline - even one they created themselves.

## Valid Transactions

The valid transactions for Dimensions RM entities are listed in the following table.

Transaction	Definition
<b>Attribute Transactions</b>	
Update	The user can change the attribute value.
<b>Board Transactions</b>	
Create Public	The user can create public boards and dashboards.
<b>Category Transactions</b>	
Category Assignment	The user can grant or revoke access to the category for groups and users for the category the group or user with this right is assigned to.
Define List Values	The user can add, or delete list entries for the category the group or user with this right is assigned to.
FullAccess	For users, for internal use only. For groups, the users in the group have instance level permission to move or copy scripts, and traceability reports into other categories, and move requirements between categories, even if they are not in a group that has permissions to the individual categories. For information about assigning groups permissions to individual categories, see " <a href="#">Assigning Categories</a> " on page 221. <b>NOTE:</b> To add, delete, rename, or move categories, users must be in the Administrator's group. The FullAccess transaction has no effect on the ability to perform these actions.
Maintain Sub-Categories	The user can create, rename, activate, inactivate, or move (by drag and drop) categories under the category the group or user with this right is assigned to.
<b>Class Transactions</b>	

<b>Transaction</b>	<b>Definition</b>
CMLock	The user can lock class objects for configuration management purposes.
Create	The user can create new class objects.
CreateCR	The user can create new change requests for class objects.
Delete	The user can mark class objects as deleted.
Execute Transition	The user can execute any transition of any class.
Execute Transition if Owner	The user can execute any transition if he or she owns the requirement.
Execute Transition if Submitter	The user can execute any transition if he or she submitted the requirement.
ExecuteCR	The user can accept or reject change requests.
Expand	The user can expand class objects.
Focus	The user can focus class objects.
Link	The user can create generic links to class objects.
Provide To	The user can branch requirements.
Read	The user can read class objects.
Remove	The user can remove class objects.
Replace	The user can replace class objects.
Replace If Owner	The user can replace class objects if he or she owns them.
Synchronize To	The user can merge branched requirements.
Undelete	The user can undelete class objects.
Unlock	The user can unlock class objects.
Update	The user can update objects with a status of "Current."
Update If Owner	The user can update objects with a status of "Current" if he or she owns them.
UpdateCR	The user can update an object with a status of "Proposed."
UpdateNonCurrent	The user can update objects where the status is not "Current."
<b>Collection Transactions</b>	
Associate to a Dimensions CM Project	The user can associate a collection with a Dimensions CM project.
Create	The user can create a new collection.
Create Based on Existing Collection	The user can create a collection based on an existing collection.
Create Baseline	The user can create a baseline from a collection.
Delete	The user can delete collections.
Link	The user can add requirements to collections or remove requirements from collections.

Transaction	Definition
Link Requirement to Dimensions CM Project	The user can add a requirement to a collection that is associated with a Dimensions CM project.
Remove	The user can remove a collection.
Remove Baseline	The user can remove baselines.
Rename Baseline	The user can rename a baseline.
Undelete	The user can undelete collections.
Update	The user can create/edit alias's and modify parent/child links for a collection.
<b>Document Transactions</b>	
Create	The user can create a new document.
Create Based on Existing Document	The user can create a new document which uses an existing document as a template.
Create Snapshot	The user can create snapshots.
Delete	The user can delete documents.
Delete Snapshot	The user can delete snapshots.
Full Snapshot Access	The user can read requirements and chapters and add comments, even if they do not have access to the category where the requirements exist. The user <b>does not</b> have access to the snapshot if he or she cannot access the category the snapshot resides in.
Link	The user can add chapters and requirements to a document and edit sub-chapters.
Manage Parent Document	The user can create and manage parent documents.
Remove	The user can remove documents.
Remove Snapshot	The user can remove snapshots.
Rename Snapshot	The user can rename snapshots.
Undelete	The user can undelete documents.
Unlock	The user can unlock documents.
Update	The user can edit the root chapter of a document.
Update Properties	The user can modify document properties.
<b>Import Transactions</b>	
Import	The user can import documents and requirements.
<b>Relationship Transactions</b>	
Clear Suspect Links	The user can clear suspect links of one requirement at a time.
Create	The user can create new links for relationships.
Delete	The user can delete links for relationships.
Mass Clear Suspect Links	The user can delete suspect links of one or several requirements at a time.
Modify	The user can change relationship attribute values.

Transaction	Definition
Raise Suspect Links	The user can make a linked requirement suspect.
Read	The user can look at relationship links.
Remove	The user can remove relationship links.
Undelete	The user can undelete relationship links.
<b>Report Transactions</b>	
Create	The user can create new reports. <b>NOTE:</b> If you do not have Create permission, you can create a new report; however, you cannot save it.
Create Public	The user can create new public reports.
Read	The user can see and execute reports.
Remove	The user can remove reports.
Rename	The user can rename reports.
Update	The user can change reports.
<b>User Transactions</b>	
Team Maintenance	The user can create, edit, and delete Agile teams.
User Group Assignment	The user can assign users to groups.

## Database Password Encryption

As of release 25.2 (13), database passwords are encrypted by default using the AES encryption algorithm. Password encryption is no longer the responsibility of the System Administrator.

## Managing Databases

In the Dimensions RM environment, a database represents an instance of Oracle. The database can contain multiple Dimensions RM instances. The databases that are displayed are determined by the contents of the `tnsnames.ora` file.

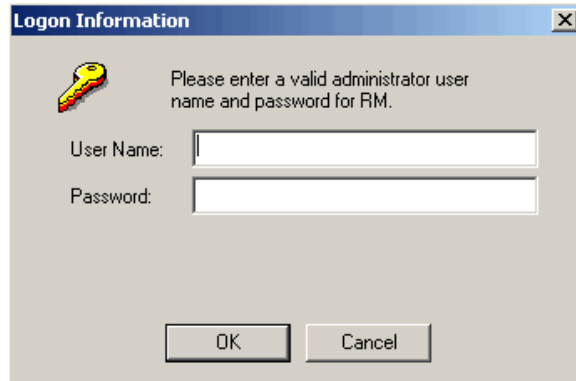
Before you can access the instances contained in a database, you must first log on using a valid Dimensions RM user and password. Once you have been validated, the instances that you are able to administer will be available. The list of users and groups is defined once for a database and is shared across all instances contained within that database.

You can have any number of Dimensions RM instances in the your own company's database. When you create an instance, you can import data from a saved instance or create a "blank" instance. Dimensions RM allows you to choose the size of the tablespace datafile, which is a unit of storage where data is physically stored. You also can convert a database from a previous version of Dimensions RM.

## Logging onto a Database

### To log on to a database:


- 1 In **RM Manage**, select a database or expand the database folder.  
The **Logon Information** dialog box opens.



- 2 Enter an administrator user name and password.
- 3 Click **OK**.

## Logging on as a Different User

### To log on as a different user:

- 1 In **RM Manage**, select the database to which you want to log on.
- 2 Select **File | Change User**, click the **Change User** button , or right-click the database and select **Change User**.
- 3 Enter the new user name and password and click **OK**.

## Converting a Database or Instance

The conversion tool allows you to upgrade older versions of a Dimensions RM instance database to the current version. If you upgrade Dimensions RM to take advantage of improved features, you must convert the database and instances.




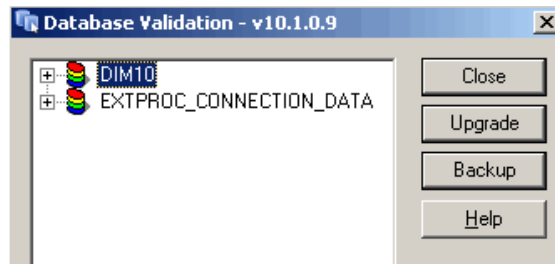
**IMPORTANT!** Before you upgrade any instance, ensure that you have a recent backup, see "[Dimensions RM Backup](#)" on page 182. The backup must be created with the version that was used for creating the original RM instance. The backup file should be kept in your archives.

During the upgrade, the instance is incrementally converted until it gets to the current version. This will take some time as table structures and stored procedures within the instance area are modified.

### To convert a database or instance:

- 1 In **RM Manage**, select the database that contains the instance you want to convert.

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



- 3 To expand the database that contains the instance you want to convert, click +.
- 4 Enter the ICDBA password.
- 5 Select the instance and click **Upgrade**.
- 6 To start the upgrade, click **Continue**. The upgrade may take several minutes to complete.



#### NOTES

- The Document View perspective in RM Browser requires title and description attributes. When you upgrade an instance that does not have a title and description attribute set for each class, a message is displayed that informs you that the upgrade process will add attributes if no existing attributes are acceptable.

After you upgrade, review each class and class type and, if necessary, select or create more appropriate attributes to use for the title and description.

The upgrade process could select an implicit attribute such as *Created by* for the title or description attribute. If a Class Definition diagram includes an implicit attribute for the title or description attribute, you must change the attribute to a user-defined attribute, or you will be unable to save the Class Definition diagram. If an appropriate user-defined attribute does not exist, you must create one.

For information about setting the title and description attributes, see "[Specifying Attributes](#)" on page 304. For more information about Document View, see the *Dimensions RM Browser User's Guide*.

- The upgrade process detects any non-unique attribute name and prompts you for a new name. For example, the upgrade process prompts you for a new name for a user-defined attribute named *Category* and changes the attribute name to the new name. This is done to prevent a conflict with a user-defined attribute named *Category* and the implicit attribute named *Category*.

- 7 When the resources have been updated, click **Close** to exit the conversion tool.


## Administering Tablespaces

A tablespace is a logical storage unit. Each instance is physically stored in one or more data files associated with a tablespace. Initially, only one file is associated with the tablespace, but you can add more files as you need them.

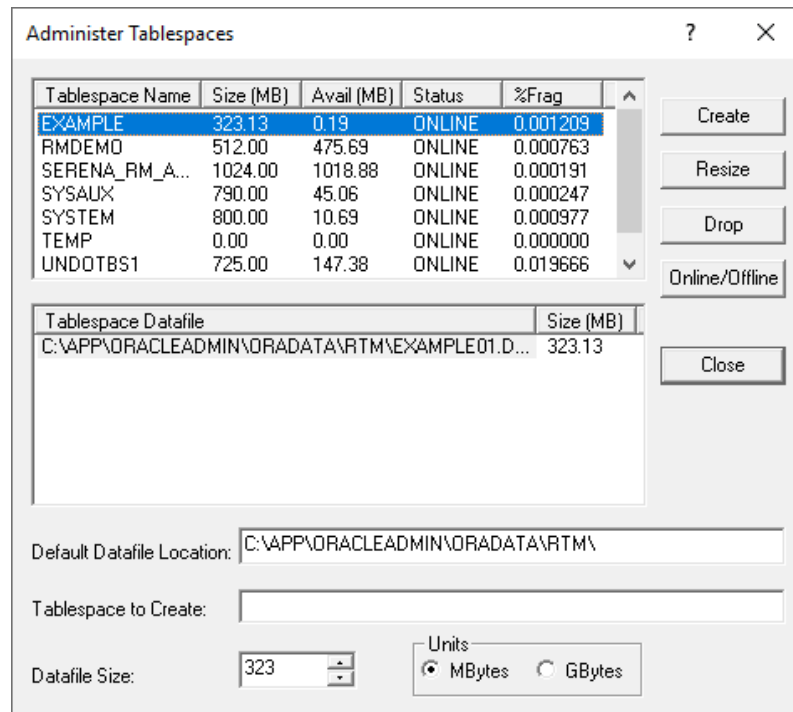
The size of the tablespace is determined by the size of the data file or combined data files that make up the tablespace.

## Creating a Tablespace

### To create a tablespace:

- 1 In **RM Manage**, select the database in which you would like to create a tablespace.
- 2 Select **File | Administer Tablespaces**, click the **Administer Tablespaces** button , or right-click the database and select **Administer Tablespaces**.
- 3 If prompted, enter the ICDBA password and click **OK**.

The **Administer Tablespaces** dialog box opens.




- 4 Enter a name in **Tablespace to Create** for the tablespace.
- 5 In the **Datafile Size** field, enter or select a datafile size.
- 6 Select a unit for the size. You can choose megabytes or gigabytes.
- 7 Click **Create**.

## Dropping a Tablespace

When you drop a tablespace, the tablespace and all data in it are deleted.

### To drop a tablespace:


- 1 In **RM Manage**, select the database in which you would like to drop a tablespace.
- 2 Select **File | Administer Tablespaces**, click the **Administer Tablespaces** button , or right-click the database and select **Administer Tablespaces**.
- 3 If prompted, enter the ICDBA password and click **OK**. The **Administer Tablespaces** dialog opens.
- 4 Select the tablespace you want to drop from the top list.

- 5 Click **Drop**.
- 6 Click **Yes** to confirm the deletion when prompted.

### ***Resizing a Tablespace***


You can resize a tablespace when you are running low on available space. In general, you should consider increasing tablespace when available space is about 5 MB. How much you resize the tablespace varies, depending how much work you intend to do, how much disk space is available, and at what stage you are in your instance.

#### **To resize a tablespace:**

- 1 In **RM Manage**, select the database in which you would like to resize a tablespace.
- 2 Select **File | Administer Tablespaces**, click the **Administer Tablespaces** button , or right-click the database and select **Administer Tablespaces**.
- 3 If prompted, enter the ICDBA password and click **OK**. The **Administer Tablespaces** dialog box opens.
- 4 Select a tablespace in the top list.
- 5 If you want to resize an existing tablespace file, select the file in the bottom list. If you want to create another tablespace file, do not select anything in the bottom list.
- 6 Click **Resize**. You will be asked if you want to resize an existing tablespace file. Select **Yes** if you want to resize an existing tablespace file; otherwise a new tablespace file will be created.


### ***Placing a Tablespace Online or Offline***

#### **To place a tablespace online:**

- 1 In **RM Manage**, select the database which you would like to place online or offline.
- 2 Select **File | Administer Tablespaces**, click the **Administer Tablespaces** button , or right-click the database and select **Administer Tablespaces**.
- 3 If prompted, enter the ICDBA password and click **OK**. The **Administer Tablespaces** dialog box opens.
- 4 Select an offline or online tablespace in the top list.
- 5 If you want to place the tablespace online, select the file in the bottom list. If you want to create another tablespace file, do not select anything in the bottom list.
- 6 Click **Online/Offline**.

### ***Setting Default Location for Tablespace***

#### **To set the default location for a tablespace:**

- 1 In **RM Manage**, select the database in which you would like to set a default tablespace location.
- 2 Select **File | Administer Tablespaces**, click the **Administer Tablespaces** button , or right-click and select **Administer Tablespaces**.

- 3 If prompted, enter the ICDBA password. The **Administer Tablespaces** dialog box opens.
- 4 Enter a location in the **Default Datafile Location** box.

## Configuring E-Mail Notification

The RM Mail service is designed to provide an automated mechanism for sending e-mail to registered users when a user-defined set or criteria is matched by an object in the database. The functionality is implemented in three different segments:

- **Mail Service**—At least one Windows machine on the network must be configured to run the RM Mail service. RM Mail monitors the selected instances and dispatches e-mails as the specified criteria are met. Note that a single instance of RM Mail can monitor multiple instances on multiple database locations.
- **RM Mail Configuration** —The system on which RM Mail is installed has a Windows applet used to configure the various aspects of the mail service.
- **Rule Configuration**—Instance administrators and users configuration the notification rules in the RM Browser application.



**NOTE** Some e-mail clients modify the formatting of incoming e-mail messages by removing what they consider "extra" formatting. To prevent this, disable the options in your e-mail client that cause this modification.

### To configure the RM Mail service:

- 1 Select **Programs | Open Text | Dimensions RM version | RM Mail Configuration** from the Windows **Start** menu. The RM Mail configuration applet starts.

The **RM Mail** dialog box has these tabs:

- **Database:** Used to select the database location and instances that the mail service should monitor (see "[Database Tab](#)" on page 241).
- **Mail Service:** Used to specify the name of the SMTP mail server to be used for sending mail, as well as the name and e-mail address from which the e-mail should be sent (see "[Mail Server Tab](#)" on page 242).
- **Control:** Used to start and stop the e-mail service, as well as specify the interval at which the service should run (see "[Control Tab](#)" on page 243).
- **Log:** Used to configure the amount of log information that is appended to the system application log (see "[Log Tab](#)" on page 245).
- **Notifications:** Used to inform administrators about administrative activities, e.g. creation of users or groups (see "[Notifications Tab](#)" on page 245).
- **General:** Used to specify the RM Browser URL for RM Mail service (see "[Log Tab](#)" on page 245).

- 2 Specify RM mail settings.
- 3 Click **Apply**.
- 4 Stop and then restart the **Dimensions RM E-Mail Service** service.

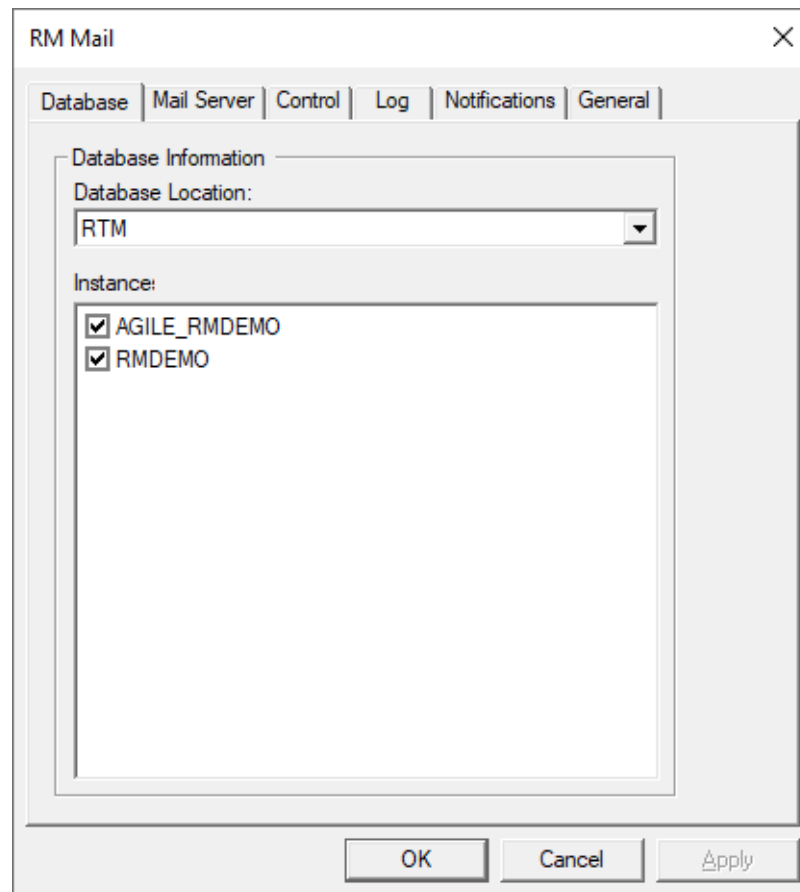
This can be done from the following locations:

- RM Mail **Control** tab (see "[Control Tab](#)" on page 243)
- Windows **Services** (from the Windows **Control Panel**, double-click **Administrative Tools** and then double-click **Services**).

## Database Tab

First, choose the database, if running this app on the server, the database names should appear on the drop-down under Database Location.

Once the database location is selected, a list of all Dimensions RM instances available is displayed.



In the check box next to each instance, select the instances this service should monitor. The mail service can monitor multiple instances at many locations.

**Disabling e-mail notifications for an instance does not delete the rules that have been defined for the instance. It simply informs the RM Mail service to ignore them.**



**NOTE** It is reasonable to disable notifications when performing very large update/import tasks so users are not inundate with email messages.

## Mail Server Tab

For the RM Mail service to send e-mail, it must have access to an SMTP mail server available on your network. For this and all client server communications, we recommend using TLS.

Fill the fields of the dialog as required or desired:

Field	Description
<b>Server Name (SMTP):</b>	The name or IP address of the SMTP server
<b>Server Port:</b>	The port used for communication with the SMTP server; 25 is the default.
<b>Use TLS:</b>	If enabled, TLS security will be used. For secure communication, TLS is recommended.
<b>Use Authentication:</b>	Enable this option, if the SMTP server requires a user name and password.
<b>Authentication Mode:</b>	The authentication mode depends on the SMTP server. <ul style="list-style-type: none"> <li>■ <b>Login:</b> Transmits user name and password individually.</li> <li>■ <b>Plain:</b> Transmits user name and password together.</li> </ul>
<b>Login:</b>	A user name that is accepted by the SMTP server.

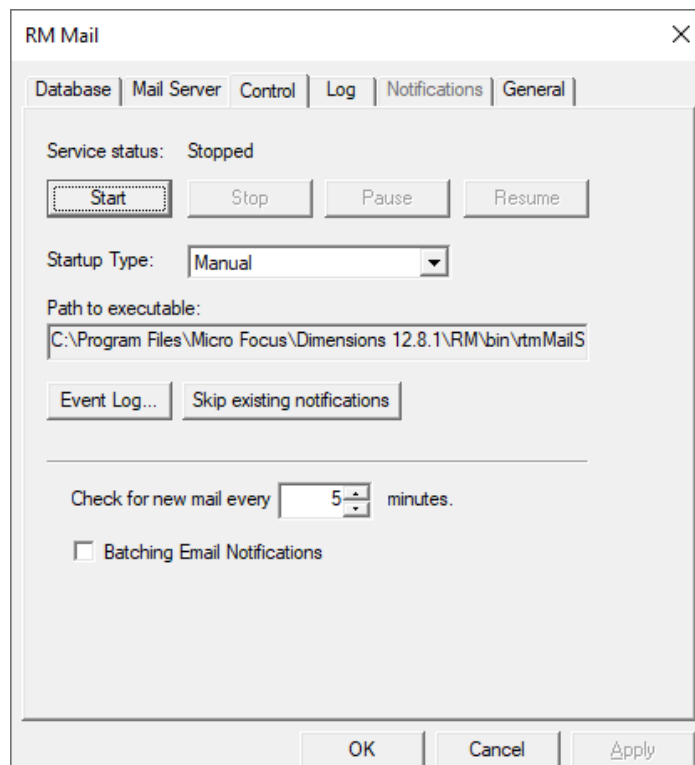
Field	Description
<b>Password:</b>	The password for the SMTP user name.
<b>Name:</b>	Specify the name you want users to see as the sender's name, e.g. <i>Dimensions RM Administrator</i> . If replies are not wanted, leave this field blank.
<b>E-Mail Address:</b>	Specify the e-mail address you want users to be able to reply to. If replies are not wanted, leave this field blank.

### To test your configuration, do the following:

- 1 Click **Send test email**. This opens the **Send Test Email** dialog.
- 2 Enter an e-mail address to which the test e-mail will be sent.
- 3 Click **OK** to send the test e-mail.

## Control Tab

The control tab provides a simple way to control the status of the RM Mail service.



The current status of the service is displayed at the top of the dialog box.

To save changes made to the configuration before starting the RM Mail service, click **Apply**. To start the service, click **Start**. To stop the service, click **Stop**.

The **Startup Type** drop-down list provides three options:

- **Automatic**—The service is started automatically at system boot time.

- **Manual**—The user must start the service manually, either from the RTM Mail Configuration applet or the Services applet on the control panel.
- **Disabled**—The service cannot be started either automatically or manually.



**NOTE** The service can also started and stopped from Windows **Services** (from the Windows **Control Panel**, double-click **Administrative Tools**, and then double-click **Services**).

The interval at which the mail service should process the e-mail rules can be selected by changing the value for the **Check for New E-mail** field. The default value for this field is 5 minutes, although the actual value used depends on the number of changes being made to the instance data and maximum acceptable delay between a change occurring and the e-mail being sent. Generally, the more operations that are being performed on the data, the shorter the interval should be.

### ***Removing Unsent E-Mail Notifications from the Mailing Queue***

If the RM Mail service has been disabled for a long time and the e-mail notifications were still active, or you just disabled RM Mail service and e-mail notifications, you should remove unsent e-mail notifications from the mailing queue. This prevents that when you reactivate the RM Mail service old notification e-mails are sent to users.

#### **To remove unsent e-mail notifications, do the following:**

- 1 Ensure that on the **Database** tab, database and at least one instance have been selected.
- 2 On the **Control** tab, click **Skip existing notifications**.
- 3 Confirm the warning message by clicking **OK**.
- 4 Click **OK** to close the success message.

### ***Combining Notifications into a Single E-Mail***

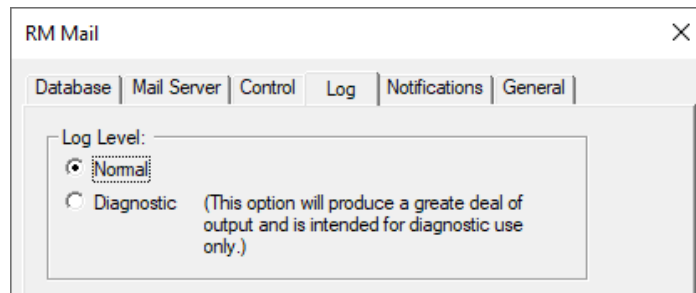
In order to remove stress from the mail server and avoid users to receive a lot of notification e-mails, all user notifications for the same class can be combined into a single e-mail. To increase the chance to combine notifications into one e-mail, ensure that the value of the **Check for new mail every ... minutes** is not too small.

#### **To combine notifications into one e-mail, do the following:**

- 1 Ensure that on the **Database** tab, database and at least one instance have been selected.
- 2 On the **Control** tab, select **Batching Email notifications**.
- 3 Set the value for **Check for new mail every ... minutes** to a convenient value. For receiving one combined e-mail per day, set the value to 1440.
- 4 Click **Apply** to accept your changes.
- 5 Restart the RM Mail service by clicking **Stop**, followed by **Start**.

## Log Tab

The RM Mail service writes information to the system application log to inform the user of events that have happened. The **Log** tab allows you to specify the log level.

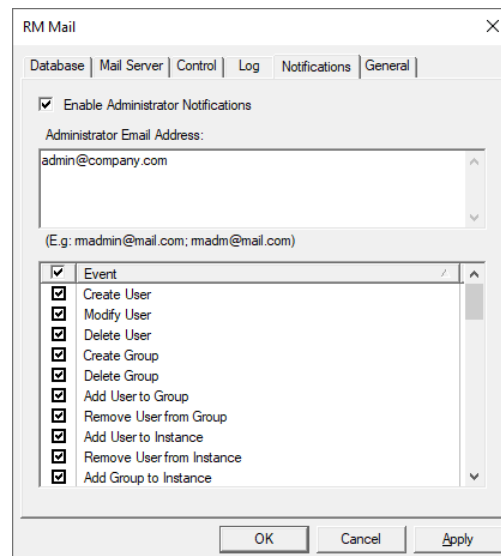


The default log level is **Normal**, which logs a minimum of information to the system application log and is the recommended option for normal use.

The **Diagnostic** option helps locate problems that might occur and logs every operation that the RM Mail service performs. This generates much information in the system application log, which could fill the log. When running in verbose mode, it is recommended that the application log be configured to overwrite older events to avoid generating warning messages by the operating system.

## Notifications Tab

Please Note that notifications should be created by the Instance Administrator in the Browser. See "Managing Notifications" in the **RM Browser User's Guide**.



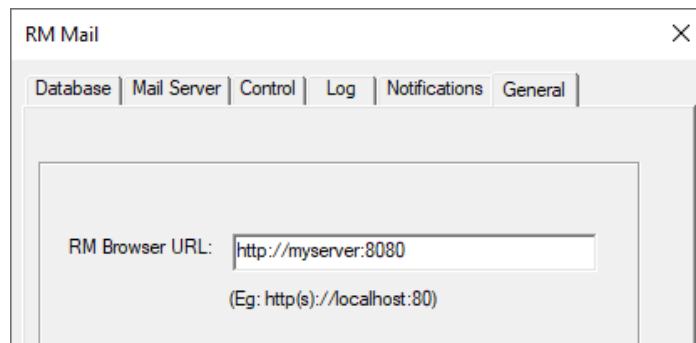
**The following options are available:**

- Enable Administrator Notifications:** Enables the function to send e-mails when system events occur.

- **Administrator Email Address:** Enter the e-mail address to which you want to send the notifications to. If you want to specify several e-mail addresses, separate them with a semicolon.
- **Event:** Select the events for which you want to receive notifications. By default, all events are subscribed. You can toggle subscription for all events by clicking the check box on the table header.

## General Tab

The **General** tab is used to specify the RM Browser URL for RM Mail service.



## Login Sources

Dimensions RM supports multiple login sources, including:

- **LDAP:** Lightweight Directory Access Protocol. Use this source to authenticate user IDs and passwords against an LDAP server.
- **SSO:** Single Sign On. Use this source to authenticate users against a Open Text SSO server (the Open Text SSO server is an optional part of Dimensions CM and SBM installations, not a part of Dimensions RM). SSO streamlines login across the products and within RM. It also enables CAC (Common Access Card) authentication.



**NOTE** Before you can use SSO with your RM clients, you must configure the RM server to connect to the Open Text SSO server. See the *Dimensions RM Installation Guide*.

- **RM:** Use this source to authenticate user IDs and passwords that are stored in Dimensions RM.
- **AZURE AD:** Azure Active Directory allows organizations to verify user accounts against Microsoft's cloud based directory and identity management service. This is especially useful if you want to grant access to Dimensions RM for users outside your corporate domain.
- **SAML SSO:** Security Assertion Markup Language (SAML) enables organizations to verify user accounts using the SAML authentication standard.

You can specify that multiple sources be used to authenticate users, and specify the order in which they should be used. If multiple sources are specified and the first login attempt

fails because the user is not found, Dimensions RM looks for the user in the next enabled source. For the LDAP source, you can specify multiple LDAP servers and their order. A new Dimensions RM user can be automatically created after a user has been authenticated against LDAP or SSO, if so configured.



**NOTE** If the login fails due to an invalid password, no attempt is made to authenticate against the next login source.



**IMPORTANT!** Each user ID is valid for only ONE login source.

- To allow a user the ability to login from two different login sources, you must create two unique user IDs for that user, one for each login source. For example: JohnS\_sso and JohnS\_ldap.
- Once a user ID is created, the login source associated with it cannot be changed. If you manually create a user ID with RM Manage, that user ID will only work with the RM login source. If a user ID is auto created in RM by an external login source (LDAP or SSO), that user ID will only work with the login source that created it.

The following steps describe the process that takes place when LDAP is used as a login source:

- 1 The user's credentials are authenticated against the LDAP server.
- 2 The user's LDAP user name is used to log the user into Dimensions RM. If a password is stored for the user in Dimensions RM, it is ignored.
- 3 If the user does not already exist in Dimensions RM, the user is created using specified criteria (this is optional).



**NOTE** The group and instance to be associated with new users must be set up before configuring LDAP as a login source.


## Specifying Login Sources in RM Manage

You can specify multiple login sources, or just one of them. You can also change the order in which the sources are used to authenticate users.

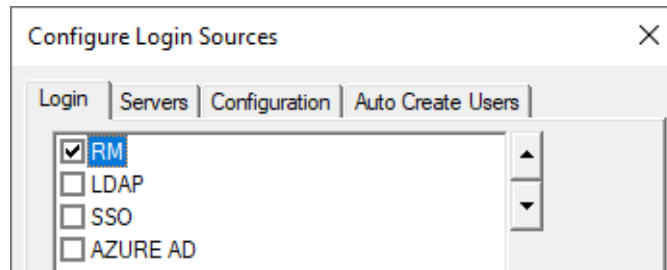


**NOTE** Deselecting the SSO login source does not disable the configuration changes that were made during the installation of the SSO components. See ["Fully Disabling SSO" on page 251](#).

**To specify login sources:**

- 1 In **RM Manage**, select the database for which you want to set login sources.
- 2 Select **File | Configure Login Sources**, and click the **Configure Login Sources** button , or right-click the database and select **Configure Login Sources**.

- 3 Enter the password for the ICDBA account if prompted to do so. The **Configure Login Sources** dialog box opens.



- 4 Select the login sources that you want Dimensions RM to use.
- 5 Use the up and down arrow buttons to change the order of the sources. The order that you define here is the order in which Dimensions RM attempts to authenticate users.



**IMPORTANT!** Each user ID is valid for only ONE login source.

- To allow a user the ability to login from two different login sources, you must create two unique user IDs for that user, one for each login source. For example: JohnS\_sso and JohnS\_ldap.
- Once a user ID is created, the login source associated with it cannot be changed. If you manually create a user ID with RM Manage, that user ID will only work with the RM login source. If a user ID is auto created in RM by an external login source (LDAP or SSO), that user ID will only work with the login source that created it.


- 6 If you selected...
  - **RM:** If you did not select any other login source, click **OK**.
  - **LDAP:** Proceed to ["Specifying an LDAP Server" on page 252](#).
  - **SSO:** Note that before you can use SSO with your RM clients, you must configure the RM server to connect to the Open Text SSO server. See the *Dimensions RM Installation Guide*. To automatically create users on their first SSO login, see chapter ["Creating RM Users Automatically" on page 248](#).
  - **AZURE AD:** ["Retrieving Configuration Data from Azure AD" on page 525](#)
  - **SAML SSO:** ["Azure SAML2 Authentication" on page 528](#)

## Creating RM Users Automatically

Optionally, you can specify whether RM users are automatically created when a new SSO or LDAP authenticated user logs in.



**NOTE** Before you can use SSO with your RM clients, you must configure the RM server to connect to the Open Text SSO server. See the *Dimensions RM Installation Guide*.

- 1 If the **Configure Login Sources** dialog box is not already open, do the following:
  - a In **RM Manage**, select the database for which you want to configure SSO.
  - b Select **File | Configure Login Sources**, click the **Configure Login Sources** button , or right-click the database and select **Configure Login Sources**.

- c Enter the password for the ICDBA account if prompted to do so.

The **Configure Login Sources** dialog box opens.

- 2 Select the **Auto Create Users** tab.

Configure Login Sources

Login | Servers | Configuration | **Auto Create Users**

Auto create users for LDAP/SSO login

Get user group from attribute

Map external group to RM group

Instance:

Assign users to groups:

	Group Name	External Group	Assign to Category
<input type="checkbox"/>	Administrators		<input type="checkbox"/>
<input checked="" type="checkbox"/>	BUSINESS_ANALYST	RM_BusinessAnalyst	<input checked="" type="checkbox"/>
<input type="checkbox"/>	icDemo Users		<input type="checkbox"/>
<input type="checkbox"/>	MANAGER		<input type="checkbox"/>

OK Cancel Help

- 3 **Auto create users for LDAP/SSO login:** Select this option to automatically create user IDs in Dimensions RM for users authenticated through SSO or LDAP.
- 4 **Get user group from attribute:** Select this option to specify an LDAP attribute that provides the group(s) to assign the user to when creating the account.
- 5 **Map external group to RM group:** Select this option if the LDAP groups differ from the groups in Dimensions RM. This shows the **External Group** column in the **Assign users to groups** table.
- 6 **Instance:** Select the instance to which you want to assign the automatically created user.
- 7 **Assign users to groups:**
- Select the option left of the group name to assign an automatically created user to this group.

- **External Group:** This column is only available if you selected the **Map external group to RM group** option. To specify an external group, double-click into the column and specify one or several group names. You can separate group names with a semicolon. You can either use the display name of a group, e.g. *RM\_BusinessAnalyst*, or the full name, e.g. *CN=RM\_BusinessAnalyst,OU=Sales,DC=mydomain,DC=com*. The full name should be used if the groups are ambiguous.



**CAUTION!** Group assignments are synchronized at login. This means that if a user has been manually removed from a group, he will be added again if he is assigned to that group in LDAP.

- **Assign to Categories:** By selecting the option in this column, the user is assigned to all categories this group has access to. If this option is clear, you have to assign users manually either in RM Manage (see chapter "Assigning Categories" on page 221) or in RM Browser (see chapter "Managing Access Rights" in the *Dimensions RM Browser User's Guide*).

8 Click **OK**.

## Changing the SSO Provider Host Name

If your SSO installation is moved to another host, you need to change the SSO configuration files to be able to log on to Dimensions RM.

**To change the SSO provider host name, follow these steps:**

- 1 Change the redirection of web client login:
  - a On the RM server, open the following file in a text editor:  
*RM\_Install\Common Tools \#.#\tomcat\#\#\alfssogatekeeper\conf\gatekeeper-core-config.xml*
  - b Change protocol (http or https), host name and port to match the new server connection for the parameter tags with these names:
    - SecurityTokenService
    - SecurityTokenServiceExternal
    - FederationServerURL
  - c Save the file.
  - d Restart **Dimensions RM Common Tomcat** service.
- 2 On systems using remote fat clients to access the RM server via SSO do the following:
  - a Open a registry editing application (select **Run**, enter `regedit`, and click **OK**).
  - b Navigate to one of the following:  
`HKEY_LOCAL_MACHINE\SOFTWARE\Micro Focus\Dimensions RM\Environment\Default`
  - c Change Registry value **SSOserver** to match protocol, host name and port of the new connection.
  - d Change Registry value **SSO\_HOST** to match the new SSO host name.

- e Change Registry value **SSO\_PORT** to match the new SSO port.



**NOTE** After changing the SSO host name it might become necessary to import the certificate with the new host name. For more information about importing refer to chapter "SSO and CAC Configuration" in the *Dimensions RM Installation Guide*.

## Fully Disabling SSO

When you install the Single Sign On (SSO) components, changes are made to certain configuration files and registry entries. Deselecting the SSO login source in the Configure Login Sources dialog does not undo the configuration changes that were made during installation of the SSO components.

### To disable SSO follow these steps:

- 1 Deselect the **SSO** login source via the Configure Login Sources dialog. See "[Specifying Login Sources in RM Manage](#)" on page 247.

- 2 Disable the redirection of web client login:

- a On the RM server, open the following file in a text editor:

```
RM_Install\Common Tools
#. #\tomcat\#. #\conf\alfssogatekeeper\conf\
gatekeeper-services-config.xml
```

- b Comment out all lines where the **requestURI** attribute contains `/rtmBrowser/`. Examples:

- `<URIMatcher requestURI="/rtmBrowser/*"/>`
- `<URIMatcher requestURI="/rtmBrowser/css/*"/>`



**NOTE** To comment out an XML section, use the `<!--` and `-->` statements, for Example: `<!--<URIMatcher requestURI="/rtmBrowser/*"/>-->`

- c Save the file.

- d Restart **Dimensions RM Common Tomcat** service.

- 3 Remove the SSO registry key on systems using remote fat clients to access the RM server via SSO:

- a Open a registry editing application (select **Run**, enter `regedit`, and click **OK**).

- b Navigate to one of the following:  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Micro Focus\Dimensions RM\Environment\Default

- c Delete the **SSOserver** key.



**TIP** Make a note of the registry key and its value in case you want to restore it in the future.


- d Close the registry tool.

- 4 Restart the RM server.

## Specifying an LDAP Server

If you plan to use LDAP as a login source, you must specify one or more LDAP servers.

### To specify an LDAP server:

- 1 If the **Configure Login Sources** dialog box is not already open, do the following:
  - a In **RM Manage**, select the database for which you want to specify an LDAP server.
  - b Select **File | Configure Login Sources**, click the **Configure Login Sources** button , or right-click the database and select **Configure Login Sources**.
  - c Enter the password for the ICDBA account if prompted to do so.  
The **Configure Login Sources** dialog box opens.
- 2 Click the **Servers** tab.
- 3 To add a server to the **LDAP Servers** list, complete the following fields:
  - a **Server Name:** Enter the host name or IP address of the LDAP server. For example, `myserver.mydomain.com`
  - b **Server Port:** Enter the port number of the LDAP server. LDAP servers are typically configured to use port 389 (no Secure Socket Layer (SSL)) or 636 (SSL).
  - c **Add:** Click to add the server to the **LDAP Servers** list.




**NOTE** If you are using redundant servers, add each server to the list. If you are using referrals to search among unique servers, only one server is needed in the list.

- 4 Select a server in the **LDAP Servers** list and do any of the following:
  - To reposition the selected server in the LDAP Servers list, click the up or down arrow button. Dimensions RM searches for login authorization starting from the top of this list.
  - To delete the selected server from the list, click **Delete**.
  - To test the connection to the selected server, click **Test**.
- 5 Proceed to "[Specifying the LDAP Configuration](#)," next.

## Specifying the LDAP Configuration

If you are using LDAP as a login source, you must specify an LDAP configuration.

### To specify an LDAP configuration:

- 1 If the **Configure Login Sources** dialog box is not already open, do the following:
  - a In **RM Manage**, select the database for which you want to specify an LDAP server.
  - b Select **File | Configure Login Sources**, click the **Configure Login Sources** button , or right-click the database and select **Configure Login Sources**.
  - c Enter the password for the ICDBA account if prompted to do so.  
The **Configure Login Sources** dialog box opens.

- 2 Click the **Configuration** tab.

The screenshot shows the 'Configure Login Sources' dialog box with the 'Configuration' tab selected. The 'Follow Referrals' checkbox is checked. The 'Connection Timeout' is set to 30 seconds. Other fields are empty.

- 3 To enable Secure Socket Layer, select the **Use SSL (Secure Socket Layer)** check box.
- 4 To allow Dimensions RM to follow referrals from one LDAP server to another, select the **Follow Referrals** check box. Use this feature to support properly configured non-redundant distributed servers.
- 5 In the **Base User Context** field, specify the base user context (distinguished name). This is the base from which to search for users. Depending on your Active Directory configuration, you might need to do the following:
  - **All users are within the same organizational unit (OU):** Specify the whole path, e.g. *OU=Marketing,CN=mydomain,CN=com*. In this case, the **Follow Referrals** option should be turned off.
  - **Users are in different organizational units (OU):** Specify the highest possible path, e.g. *CN=mydomain,CN=com* and select the **Follow Referrals** option.
- 6 In the **User Naming Attribute** field, specify the user naming attribute. This is the attribute in which the LDAP server holds the user ID value. You can use the following values:
  - **For all users identified by Base User Context:** `sAMAccountName`
  - **For users of a certain group:**  
`(&(sAMAccountName={%s})(memberOf=CN=MyGroup,OU=Builtin,DC=mydomain,DC=com))`

Modify *CN=MyGroup,OU=Builtin,DC=mydomain,DC=com* to match the full group path in your Active Directory.

- 7 Select a method for querying the LDAP server to retrieve the list of users:
  - To query anonymously, select the **Bind Anonymously** check box. This requires that the LDAP server is configured to allow anonymous users to retrieve a list of users and attributes.



#### NOTES

- With the default configuration of Active Directory, you cannot bind anonymously to a Microsoft Active Directory Server.
  - The **User DN** and **Password** fields are disabled if the **Bind Anonymously** check box is selected.
- To require a user ID and password for queries:
    - a In the **User DN** field, specify a full user DN.
    - b In the **Password** field, specify a user password.
- 8 To set the idle time in seconds before the connection to the LDAP server times out, enter a value in the **Connection Timeout** field.
  - 9 To automatically create user IDs in Dimensions RM for users authenticated through LDAP, see chapter "[Creating RM Users Automatically](#)" on page 248.
- 10 Click **OK**.

### Example LDAP Configuration

The following illustration follows shows a typical non-SSL LDAP configuration for Microsoft Active Directory Server.

The full content of fields that are truncated in the illustration follows:

- **Base User Context**—ou=people, dc=mydomain, dc=com

- **User DN**—cn=User One, cn=Users, dc=mydomain, dc=com



**TIP** By using an LDAP browser, you can retrieve the values for **Base User Context**, **User DN** and **User Naming Attribute**. If you can log on to the LDAP server, you can use `ldp.exe`.

### Using Several LDAP Servers with Dimensions RM

Dimensions RM allows you to authenticate against several LDAP servers. This allows access of users of different domains/forests to the same Dimensions RM server.



#### IMPORTANT!

- All configured server names must be unique.
- If identical user names exist on several servers, the first server having this user name is used for authentication.

#### For using several LDAP servers, do the following:

- 1 Execute the steps to configure a single LDAP server (see chapter "[Specifying the LDAP Configuration](#)" on page 252).
- 2 Specify the related LDAP servers in RM Manage (see chapter "[Specifying an LDAP Server](#)" on page 252).
- 3 With a text editor (e.g. Notepad), create the following file:  
*RM\_Install\conf\ldap.conf*.
- 4 For each LDAP server, do the following:
  - a Specify the full server name (the server you already configured in RM Manage), surrounded by square brackets, e.g. `[ldap.server1.com]`
  - b Specify the settings (one setting per line). The following configuration for 2 servers is for reference only.
 

```
[ldap.server1.com]
USE_SSL=1
FOLLOW_REFERRALS=0
BASE_USER_CONTEXT=OU=Users,DC=server1,DC=com
USER_NAMING_ATTRIBUTE=sAMAccountName
BIND_ANONYMOUSLY=0
USER_DN=ldapquery
USER_PASSWORD=password

[ldap.server2.com]
USE_SSL=1
FOLLOW_REFERRALS=0
BASE_USER_CONTEXT=OU=Users,DC=server2,DC=com
USER_NAMING_ATTRIBUTE=sAMAccountName
BIND_ANONYMOUSLY=0
USER_DN=ldapquery
USER_PASSWORD=password
```



**NOTE** The settings match those on the **Configuration** tab of the **Configure Login Sources** dialog in RM Manage.

- **USE\_SSL: Use SSL (Secure Socket Layer).** To enable, set 1; to disable set 0.
- **FOLLOW\_REFERRALS: Follow Referrals.** To enable, set 1; to disable set 0.
- **USER\_NAMING\_ATTRIBUTE: User Naming Attribute**
- **BIND\_ANONYMOUSLY: Bind Anonymously.** To enable, set 1; to disable set 0.
- **USER\_DN: User DN**
- **USER\_PASSWORD: Password**

For reference of the above settings, refer to chapter "[Specifying the LDAP Configuration](#)" on page 252.

- 5 Save the file.

## Configuring LDAP to Use SSL

If your LDAP server is configured to use Secure Sockets Layer (SSL), but there is not a certificate database in the `LDAP_Certificates_Directory` or the database is missing the required SSL certificates, you will receive errors, such as:

```
"Failed to connect to LDAP server." or "You cannot access this
project because your login account, UserName, is invalid. . . ."
```

### Importing Certificates

In order to use SSL you need to import a public key certificate to the Trusted Root Certification Authorities on the server which runs Dimensions RM.



**IMPORTANT!** The certificate must match these requirements:

- The *Subject* field must include the fully qualified name to the LDAP server (e.g. `myldapservr.mydomain.com`).
- The *Enhanced Key Usage* (EKU) field must contain the *Server Auth* value. If the field contains `<All>`, it cannot be used for server authentication.
- The certificate must be issued from a trusted Certificate Authority, within the scope of the LDAP server or within the domain of the LDAP server.
- The certificate is valid (current date is within range of the date in the *Valid from* and *Valid to* fields).


**To import the certificate, follow these steps:**

- 1 Double-click the certificate file.
- 2 On the **General** tab, click **Install Certificate...** which opens the **Certificate Import Wizard**.

- 3 Click **Next**.
- 4 Select the **Place all certificates in the following store** option.
- 5 Click **Browse...**
- 6 Select **Trusted Root Certification Authorities**.
- 7 Click **OK**.
- 8 Click **Next**.
- 9 Click **Finish**.

### **Enabling SSL**

**To create and populate a certificate database follow these steps:**

- 1 Start RM Manage and login into the appropriate database.
- 2 Open the **Configure Login Sources** dialog box as follows:
  - a Select the database for which you want to specify an LDAP server.
  - b Select **File | Configure Login Sources**, click the **Configure Login Sources** button , or right-click the database and select **Configure Login Sources**.
  - c Enter the password for the ICDBA account if prompted to do so.

The **Configure Login Sources** dialog box opens.
- 3 Select **LDAP** as a Login Source.
- 4 Select the **LDAP Servers** tab.
- 5 For the new LDAP server, enter the appropriate details in the **Server Name** and **Server Port** fields. The default port for SSL is 636.



**NOTE** You **must** use the fully qualified server name (e.g. myldapservers.mydomain.com).

If your RM server cannot resolve the name, enter the IP address and name into the hosts file (C:\Windows\system32\drivers\etc\hosts).



**TIP** To check if your server can resolve the LDAP server name, follow these steps:

- 1 Open a command prompt.
- 2 Enter `tracert` followed by the fully qualified server name (e.g. `tracert myldapservers.mydomain.com`).
- 3 Hit Enter.

If the `tracert` command returns **Unable to resolve target system name** followed by the server name you entered, you must modify the hosts file as described above.

- 4 Click **Apply**.

- 5 Select the **LDAP Configuration** tab.
- 6 Check the **Use SSL (Secure Socket Layer)** check-box, and fill in the other data as needed for your site (see ["Specifying the LDAP Configuration" on page 252](#)).
- 7 Click **OK** to update the information within your RM instances database.
- 8 Select the **LDAP Servers** tab.
- 9 Click **Test**. You should receive the message **LDAP Test Connection successful**.
- 10 LDAP is now configured to use SSL.

## Using Two-Factor Authentication For Logins

Dimensions RM supports two-factor authentication for log-in with the RM login source. Two-factor authentication has been tested with the following apps:

- NetIQ Advanced Authenticator app
- Google Authenticator
- Microsoft Authenticator app

**To enable two-factor authentication for accounts with the RM login source, do the following:**

- 1 Open the **Login Sources** dialog (see ["Specifying Login Sources in RM Manage" on page 247](#)).
- 2 Select the **RM** login source.
- 3 Click **Settings**. This opens the **RM Login Settings** dialog.
- 4 Select **Enable two factor authentication (TOTP 2FA)**.
- 5 Click **OK** to close the **RM Login Settings** dialog.
- 6 Click **OK** to close the **Login Sources** dialog.



### NOTE

- For existing **RM** login source users, it is recommended to select the **User Must Change Password at Next Logon** option. You can change this setting either in RM Manage on the **Password** tab (see chapter ["Changing User Password Information" on page 212](#)) or in RM Browser (see chapter *"Editing a User"* in the *RM Browser User's Guide*).
- Users can add the authenticator on the Change Password page.

## Setting Up Password Security

Password security is set in the **Password Rules Settings** tab that can be accessed in the instance view.

## Setting Password Rules

Password rules are common to all user accounts. Any changes made to password settings affect all user accounts.



### NOTES

- Password rules only apply to RM user accounts (RM Login Source) for which the **Password Never Expires** option is **not selected**.
- Password rules *do not* apply to RM access using LDAP/SSO accounts.
- Password rules apply to RM databases, not to individual instances.
- Whenever a new user is created, the default password is rtm.

### To set password rules for all user accounts:

- 1 In **RM Manage**, select **View | Instances**.
- 2 Click the **Password Rules Settings** tab.
- 3 Provide entries for the following settings:

Setting	Description
eMail account for notifications	The administrator's e-mail address for users who want to contact the administrator when their account is locked.
Minimum number of characters to be changed	The minimum number of characters that users must change in their old password when creating a new one. The maximum number for this setting is 99. <b>NOTE</b> When you reset the password for an existing user, this setting is not validated.
Minimum number of digits	The minimum number of digits that a password must contain. The maximum number for this setting is 99.
Minimum number of letters	The minimum number of letters that a password must contain. The maximum number for this setting is 99.
Minimum number of uppercase letters	The minimum number of uppercase letters that a password must contain. The maximum number for this setting is 99.
Minimum number of lowercase letters	The minimum number of lowercase letters that a password must contain. The maximum number for this setting is 99.

Setting	Description
Minimum number of special characters	<p>The minimum number of special characters that a password must contain. The following special characters are allowed:</p> <p>! " # \$ % &amp; ' ( ) *  + , - _ / : ; &lt; = &gt;  ? [ \ ] ^ {   } ~ `</p> <p>The maximum number for this setting is 99.</p>
Minimum length of password	The minimum number of digits, letters, and special characters that the password must contain, based on the previous five settings. The maximum number for this setting is 99.
Minimum number of failed logins before auto disable	This is the number of allowable attempts with the wrong password before the account is locked. The maximum number for this setting is 99.
Password expiration days	The number of days until users must change their password. The maximum number for this setting is 9999.
Number of days before password expiry warning	The number of days before a password is due to expire, when users are notified of the pending expiration date and given the opportunity to change their password. A warning message is displayed every time users log in using any Dimensions RM tool. The maximum number for this setting is 999.
Number of previous passwords (history) to be stored	The number of passwords to be stored for each user. Users will not be allowed to reuse any of these passwords. The maximum number for this setting is 9999.
Number of days to store previous passwords (history)	The number of days to store any previously used passwords. When the limit is reached, the stored passwords are deleted. The maximum number for this setting is 9999.
Start date to apply password rules for on-expiring passwords.	<p>By default, unless changed as described below, password rules for non-expiring passwords will be enforced starting on 31-DEC-2099. If you do not wish for this to occur, uncheck the associated tick mark.</p> <p>Alternatively, to assign an alternative date for password rules to be enforced, either:</p> <ul style="list-style-type: none"> <li>• select and overtype, as appropriate, the day, month, and year; or</li> <li>• click the down-arrow and use the calendar dialog box that appears.</li> </ul>

**4** Click **Accept Changes**.

## ALM Integration Between Dimensions CM and Dimensions RM

The Application Lifecycle Management (ALM) integration between Dimensions CM and Dimensions RM lets you associate Dimensions RM requirements to Dimensions CM requests.

The ALM integration enables you to manage Dimensions RM requirements in Dimensions CM and, conversely, manage Dimensions CM requests in Dimensions RM. For example, when you add a requirement to or remove a requirement from a Dimensions RM container, Dimensions CM is notified with the relevant information; also, Dimensions RM baselines flow to Dimensions CM and Dimensions CM baselines flow to Dimensions RM.

In the context of an ALM integration, you can:

- Associate Dimensions RM instances a Dimensions CM products.
- Associate Dimensions RM containers (baselines or collections only) to Dimensions CM instances/streams.

See the common *Dimensions CM-Dimensions RM ALM Integration Guide* for details.

### Logging In to a Dimensions CM Server

See the common *Dimensions CM-Dimensions RM ALM Integration Guide* for details.

### Associating Dimensions RM Instances to Dimensions CM Products

See the common *Dimensions CM-Dimensions RM ALM Integration Guide* for details.

### Associating Dimensions RM Baselines or Collections to Dimensions CM Projects/Streams

See the common *Dimensions CM-Dimensions RM ALM Integration Guide* for details.

## Command Line Parameters

The Dimensions RM tools provide some command line commands that you can use for common tasks.

Tool	Action	Command
RM Manage	Launch RM Manage.	<code>icmanage -user user -password password -location database -project instance -buffer buffer -dumpfile dumpfile</code>
	Back up (Oracle database)	<code>icmanage -location &lt;database instance name&gt; -project &lt;instance name&gt; -password &lt;instance password&gt; [-buffer &lt;buffer size&gt;] -dumpfile &lt;name and path of backup file to be created&gt;</code>
	Back up (SQL Server database)	<code>icmanage -location &lt;database instance name&gt; -rmdbapassword &lt;instance password&gt; -dumpfile &lt;name and path of backup file to be created&gt;</code>
	Amazon cloud RDS mode	<code>icmanage -aws</code>  The other command line options (as described above) can be used in combination with the <code>aws</code> option.
Synch Engine	Run the Synch Engine	<code>syncengine [-f file] [-c] [-e level] [-E file] [-L priority] [-k {install config uninstall start stop}] [-n serviceName] [-v] [-h] [-p password] [-P eventName]</code>
ALF Emitter	Run ALF emitter service, see <a href="#">"Application Lifecycle Framework (ALF)" on page 145</a>	<code>ALFEventEmitter [-f file] [-c] [-e level] [-E file] [-L priority] [-k {install config uninstall start stop}] [-n name] [-v] [-h]</code>
Class Definition	Launch class definition.	<code>clasdef -user user -password password -location database -project instance</code>

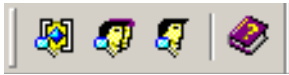
## Using RM Manage within the Amazon Cloud

Dimensions RM supports Amazon's RDS database in the AWS cloud if an Oracle database is used. To use RM Manage with an RDS database in the AWS cloud, use the `aws` option on the command line (execute `icmanage -aws`). When running RM Manage in AWS mode, the following restrictions apply:





- Tablespace cannot be administered.
- Backups of instances can only be created in legacy mode.
- Instances can only be restored in legacy mode.
- Backups of instance schemas cannot be created.
- Instance schemas cannot be restored.

# RM Manage Toolbars

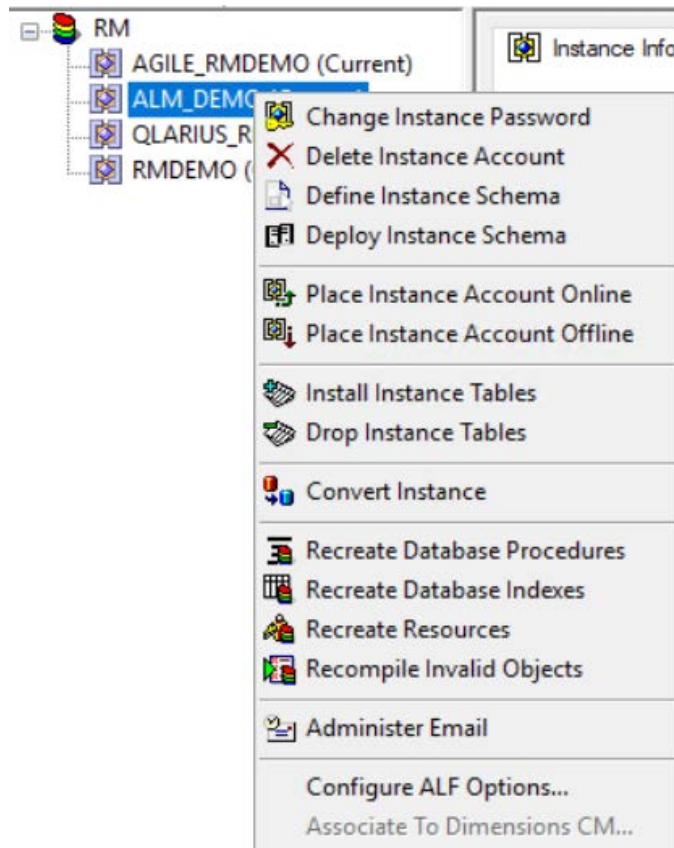
## Main Toolbar



The following table lists the buttons of the **Main** toolbar.


Button	Action
	View instance information
	View group information
	View user information
	Show Help topics

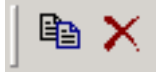
**Instance Icons:** Highlight an instance, Select **File** or right-click the highlighted instance to list available functions.





## Group Folder Toolbar




Button	Action
	New group

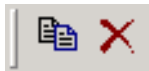
**Group Toolbar**

The following table lists the buttons of the **Group** toolbar.



Button	Action
	Copy group
	Delete group

**User Folder Toolbar**

Button	Action
	New user

**User Toolbar**

The following table lists the buttons of the **User** toolbar.

Button	Action
	Copy user
	Delete user

# Chapter 9

---

## Class Definition

Overview	266
Starting Class Definition	270
Working with the Class Definition Diagram	271
Attributes	275
Classes	298
Relationships	306
Class Types	316
Security	320
Saving the Instance Schema	323
Reloading the Instance Schema	324
Releasing the Instance Schema Lock	324
Deploying the Instance Schema	324
Printing the Instance Schema Diagram	326
Printing the Instance Schema Definitions	326
Implementing Suspect Links	327
Defining the Date Format	327
Date Format Elements	328
Date Format Element Suffixes	330
Capitalization of Date Format Elements	330
RRRR Date Format Elements	330
Punctuation and Character Literals in Date Format Models	331
Workflows	331
Creating Product and Project Classes	347

## Overview

The class definition process, referred to in the RM Browser as **Schema Definition**, provides Dimensions RM instance management.

A new instance must be defined using RM Manage (see “Managing Instances” on page 164), however most functions associated with the definition and maintenance of classes, as well as the rules and regulations governing the workflow process can be managed from RM Browser by the Instance Administrator.

A **System Administrator** will have to return to RM Manage to execute functions not yet available from RM Browser Administration:

- Copying workflows to another class (see “Copying a Workflow to another Class” on page 344)
- Schema deployment to other servers (see “Deploying the Instance Schema” on page 324)
- Define new class types or Manage Class Types (see “Class Types” on page 316)

Defining classes for an instance enables you to perform the following functions:

- Organize information according to meaningful types (classes)
- Qualify the information within each class according to attributes. This enables users to search the instance based on specific criteria.
- Maintain relationships between the classes for traceability.
- Specify the user access rights and the source documents associated with each class.

The class definition process produces the logical information model for the instance. Dimensions RM illustrates this model in a Class Definition diagram, a graphic representation of the classes and relationships you have defined. You can point-and-click to manipulate the diagram and to open associated definition windows for additions or changes.

## Defining the Instance Schema

An instance administrator can use the Class Definition tool to construct the information model for an instance in the form of a Class Definition diagram. You use the Class Definition tool to perform the following tasks:

- Define new classes; rename, modify or delete existing classes
- Define or delete attributes for each class and relationship
- Specify user access rights to each class
- Create relationships between classes
- Manipulate the class definition diagram

## Class Definition Tasks

There are three broad categories of class definition tasks:

- Instance assessment—An examination of the instance in terms of its development phases and available information.

- Class development—The definition of classes and class attributes, relationships, users and source documents.
- Process documentation—The documentation of all critical information used and decisions made throughout the class definition process.

## Modeling Instances from Project Information

Before defining classes, it is important to evaluate the type and scope of information to be modeled. The following information will help you understand your instance so that the most effective class definition model can be developed.

- Identify the type of projects that exist in your organization. Are there feasibility studies, prototypes, or full-scale development projects? This will help you determine the phasing for the projects and decide how much information needs to be modeled, where the emphasis should be placed and what kinds of reports will be needed.
- Assess the documentation and reporting requirements. They vary with the type of project and are also influenced by reports that your organization may have produced in the past. For example, for a feasibility study, risk assessment is a major issue, and you will probably want to report on high-risk components.
- Identify the customer and proprietary information that should be modeled and tracked through the successive phases of the projects.
- Assess which subsets of the information will be the most significant and/or useful.
- Consider how previous experience can assist in identifying what information needs to be modeled. You may be able to use a modified version of an existing Dimensions RM information model.
- Identify the development phases for your projects.
- Identify the information classes needed for the beginning phase, such as functional specifications.
- Identify the information classes needed for the final phase, such as test results (unit, integration and acceptance).
- Determine the required information flow between phases. This helps to identify the relationships between classes.
- Determine if some of the projects will be subcontracted to off-site development teams and requires partitioning of the information.
- Assess the detail level of the information available, and capture some basic assumptions about the structure of the information. Information assessment helps you to determine the structure of your information model as laid out in the following list:
  - **Very General:** General or summarized information, such as operational scenarios or marketing plans.
  - **High-level:** High-level information, such as system specification narratives that cover design constraints, desired features and elements that should not be included in the solution.
  - **Detailed:** Detailed information, such as subsystem specifications that provide implementation level details.

- **Low-level:** Low-level details, such as a requirement for a certain version of software or hardware.
- Assess and define the operational parameters, such as:
  - The required level of tracking among requirements, other project information, and information generated by CASE tools.
  - The members of the project teams, their responsibilities, and the access rights each will require for various types of project information during specific phases. User access rights assist you in determining which classes need to be created, which documents will be associated with each class and what is the logical breakdown of the data.

Identifying the reports that are generated helps you determine the attributes that will be needed later for searching, sorting, and printing.

## Class Definition

A class definition consists of the following components:

- A description of the class.
- The definition of attributes for the class.
- The specification of user access rights for the data assigned to the class.
- The identification of the class's relationship to other classes.

The first steps in class development are: adding classes to the class definition diagram, specifying the class types, and assigning names to each class.

The following table lists the core class types. You can create any kind class type.

Core Class Type	Description
Comment	For associating comments with objects in other class types. The comment class is particularly useful when using RM Browser, as the comment class allows users to store comments using the Internet.
ECP	For Engineering Change Proposals.
Generic	For general information (other than requirements or CASE tool data), such as acceptance test descriptions and software problem reports.
Poll	For storing polling data associated with requirements.
Requirement	For different levels of requirements information.

## Class Attributes

Attributes allow you to manage a known set of properties for each class. Attributes are distinctive pieces of information. When class attributes are present, it becomes possible for project members to search for project information based on specific criteria (specific values of the attributes).

---

## User Access to Classes

Once a class type is defined, and attributes are assigned to the class, user access rights must be defined. This determines who can access the information associated with the class. Users can be granted access at the instance level, thereby granting them access to all classes.

## Relationships Between Classes

After you have defined the classes, you can set up (and name) relationships between pairs of classes. Typically, each class is related to at least one other class. Without this connection, it is not possible to establish traceability between sets of information.

A relationship identifies how information in one class is connected to information in another class. For example, if you would like to tie a test result back to a program, you would state the relationship as "module is tested by acceptance tests." In this example, *module* is the name of the first class (also known as the primary class), *is tested by* is the name of the relationship, and *acceptance test* is the name of the second class (also known as the secondary class). This will set up the relationship between test results and modules, and enable traceability to occur between them. Engineers could then check for specific objects associated with either class.

In other words, you can retrieve information based on specific search criteria. Establishing links between objects based on certain attribute values does this. For example, a link could be created between a change request and a requirement based on the value of its approval status attribute (the values being *approved* or *disapproved*). These links are governed by the rules you set up for the relationship.

Dimensions RM relationships identify related classes. When a Dimensions RM relationship is defined, the primary class and the secondary class are identified for the relationship. A primary class can be thought of as the *source class*, and a secondary class can be thought of as the *target class*. Every RM relationship, even recursive or re-entrant relationships, must have a primary and a secondary class. In the class definition diagram, the class at the base of the relationship connector is considered the primary class. The class at the tip of the connector is considered the secondary class.

## Relationship Rules

You can set up relationship rules to govern user creation of links and determine the impact of their object edits on the relationship. For example, you can limit the number of links from one object to another, specify what should happen to an object link if the user edits the object, or only allow links based on the value of the attribute.

## Process Documentation Phase

It is important to document all critical information throughout the project assessment and class definition phases, as this information forms the basis of your instance configuration decisions and will need to reference it later. Other reasons for this documentation include:

- Referencing earlier decisions for the purpose of maintaining consistency.
- Maintaining this information for future projects.
- Helping others understand the rationale for information modeling decisions.

The following are examples of this information:

- The purpose and meaning of each class, attribute and relationship.
- A code of practice defining responsibilities for each aspect of Dimensions RM operation.
- The results and rationale for every information-modeling decision.

You can print the details of each class definition to store with your documentation.

## Attributes for Specific Classes


When users add a comment, by default, the comment dialog contains a **Role** dropdown list. You can omit this list when you define the comment class.

**To define the comment class to omit the Role menu:**

- 1 Start Class Definition (see "[Starting Class Definition](#)" on page 270).
- 2 Select a comment class on the Class Definition diagram.
- 3 Right-click and select **Define**. The **Definition of class** dialog box opens.
- 4 Click the **Attribute** tab.
- 5 In the list of attributes, under **User Defined**, double-click **Role**. The **Definition of attribute 'Role'** dialog box opens.
- 6 Click the **Core** tab.
- 7 Clear the **Attribute Editable** check box, and then click **OK**.
- 8 In the **Definition of class** dialog box, click **OK**.

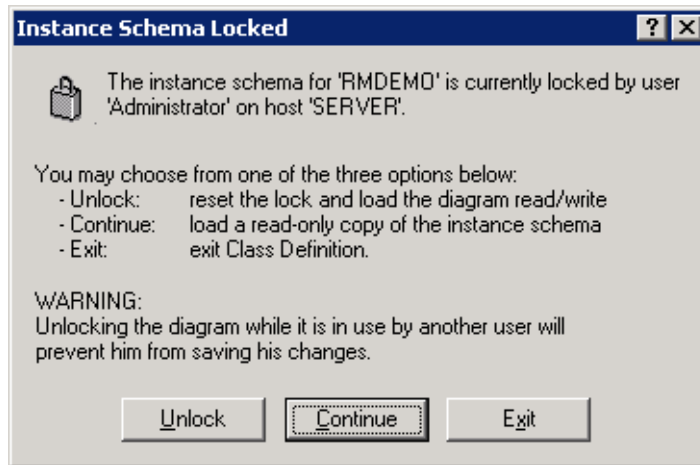
## Starting Class Definition

To start Class Definition:

- 1 Start RM Manage.
- 2 Select the instance to be configured.
- 3 Click the **Define Instance Schema** button .

If you are an instance administrator, the instance schema is launched in a Read/Write mode if another user is not currently modifying the schema. If you are an instance administrator and another user is modifying the instance schema, the **Instance Schema**

**Locked** dialog box is displayed, identifying the user currently holding the lock. A user locks an instance schema whenever it is open in read/write mode.



**Figure 9-1. Instance Schema Locked**

If you are sure the user identified is not currently modifying the instance schema, click **Unlock** to reset the lock and load the schema in read/write mode.

Alternatively, you can click **Continue** to load the schema in read-only mode or click **Exit**.



## Working with the Class Definition Diagram

The topics in this section describe how to work with the Class Definition diagram.

### Editing the Instance Header and Footer

You define the instance-wide header and footer in the Class Definition diagram. A default header and footer are created when a new instance is created.

#### To edit the header or footer:







- 1 In **Class Definition**, do one of the following:
  - Double-click the header or footer object on the canvas.
  - Select **Edit | Header** or **Edit | Footer**.
  - On the **Edit** toolbar, click the **Edit Header**  or **Edit Footer**  button.
- 2 Type the header or footer text you want in the space provided on the canvas.

If a header or footer is not required for the instance, it can be removed from the diagram by selecting the object and clicking **Delete**.

### Aligning Components

You can line up multiple components using the alignment buttons, or align a component by any edge or by its center. For a multiple selection, use the gray selection handles as

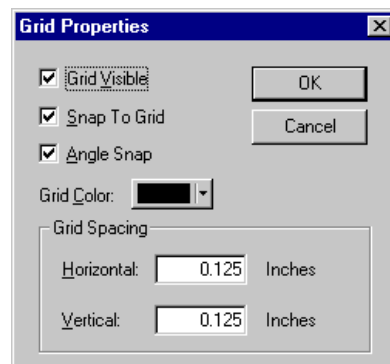
the point of reference to which components align. The following six alignment commands can be accessed from the **Alignment** toolbar or the **Drawing** menu.

-  Align Top
-  Align Middle
-  Align Bottom
-  Align Left
-  Align Center
-  Align Right

## Canvas Grid

The grid is a set of evenly spaced points on the canvas that are used to align components when they are moved. When the snap-to-grid option is enabled, the top left corner of a component is aligned to a grid point when the component is moved. The snap-to-grid feature can be enabled and disabled using by selecting **Snap to Grid** from the **View** menu. Grid visibility can be turned on and off by selecting **Grid** from the **View** menu.

To change the distance between the points of the grid, or to change the color of the grid, select **Grid Properties** from the **View** menu.



**Figure 9-2. Grid Properties**

## Centering the Diagram

**To center a diagram:**


- In **Class Definition**, select **Edit | Center Diagram** or click the **Center Diagram** button  on the **Edit** toolbar.

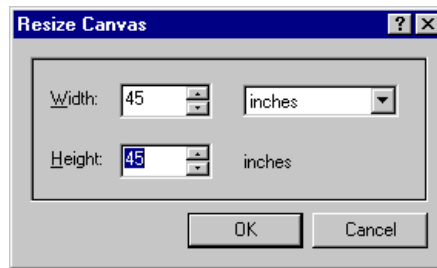
All components in the instance schema become centered, providing equal area on each side of the diagram for adding additional components.

## Changing the Canvas Size

You can resize the canvas if it is too large or too small to hold the instance schema.

**To change the canvas size:**

- 1 In **Class Definition**, select **Edit | Resize Canvas** or click the  button on the **Edit** toolbar. The **Resize Canvas** dialog box opens.



**Figure 9-3. Resize Canvas**


- 2 Enter the new width and height in the dialog box. You can enter the new dimensions in inches, millimeters, or centimeters.
- 3 Click **OK**.

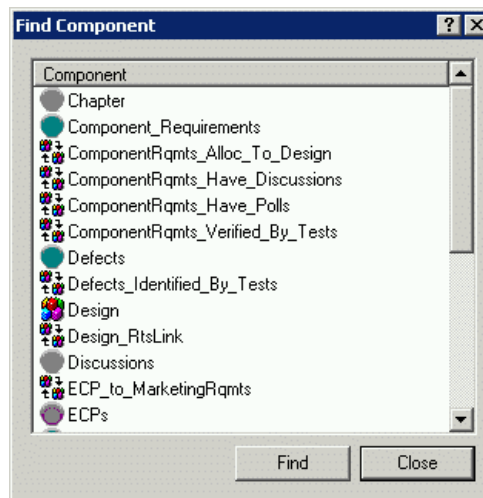
This operation may take time to complete, depending on the complexity of the instance schema. Once the schema has been resized, the components will be centered on the canvas, giving an equal amount of space on all sides to add new classes and relationships.

## Finding a Class or Relationship

A class or relationship can be located on the Class Definition diagram.

**To find a class or relationship:**

- 1 In **Class Definition**, select **Find** from the **Edit** menu, or click the **Find** button  on the **Edit** toolbar. The **Find Components** dialog box opens.







**Figure 9-4. Find Component**

- 2 Select a component and then click **Find**.

## Nudging Objects

When Class Definition is in selection mode, you can move selected components by clicking and dragging the mouse. When you place the pointer over a component that you can move, the cursor changes to a crosshair. If the **Snap to Grid** option is enabled, the top-left corner of the component's bounding box aligns with the grid.

You can move selected components by using Nudge commands. The Nudge commands move the components one unit by default and five units if you are holding the Shift key. You can access four nudge commands from the **Nudge** toolbar or the **Drawing** menu.





-  Nudge Up
-  Nudge Down
-  Nudge Left
-  Nudge Right

## Ordering Objects

The components on the Class Definition diagram can be stacked (also known as Z-order). Stacking determines where each component is drawn in the stack. In other words, the order determines which component is drawn last. The component drawn last overwrites the components already on the canvas. Z-order is determined by the order in which the components are added to the model. The last component to be added will be on top.



You can change the Z-order using order commands. The **Bring Forward** command moves a component one place in the direction of the top of the stack. The **Send Backward** command moves a component one place in the direction of the bottom of the stack. A component can be moved directly to either the top or bottom of the stack using the **Bring to Front** or **Send to Back** commands.

Each of these commands is available either from the **Structure** toolbar or the **Drawing** menu.


-  Bring to Front
-  Send to Back
-  Bring Forward
-  Send Back

## Panning the Diagram

**To pan the diagram:**

- 1 To pan to different areas of the diagram, click the **Pan** button  in Class Definition.
- 2 Click and drag the mouse to navigate the diagram.
- 3 To return to editing the diagram, click the **Select** button .

## Selecting Objects


Class Definition starts in selection mode. You can access selection mode by clicking the **Select** button .

You can select a single component by left-clicking it in selection mode. If you want to select multiple components, hold the CTRL key and then left-click each of the components you want to include in the selection, or click and drag to draw a selection rectangle. Gray selection handles distinguish the last-selected component. Class Definition uses anchor components as a reference for alignment operations. If you want another component to serve as the anchor, hold the CTRL key and click another component within the selection.


## Zooming the Diagram

The Class Definition tool provides several options for zooming.


- **Zoom to Fit**

Click the **Zoom to Fit** button  to scale the diagram such that all components on the diagram are visible in the viewport.


- **Zoom to Selection**

Click the **Zoom to Selection** button  to scale the diagram such that all selected components are visible in the viewport. To select multiple components, hold down the Shift key while clicking the left mouse button on the class or relationship you want to add to the selection. This button will only be enabled when multiple classes, relationships or both have been selected.

- **Zoom Normal**

Click the **Zoom Normal** button  to scale the diagram to its default zoom of 100%. This button will only be enabled when the diagram is zoomed other than 100%.

- **Zoom**

Click the **Zoom** button  to zoom in or out on the canvas. The pointer becomes a magnifying glass when you place it in the client area. In zoom mode, you can click the left mouse button to zoom in or the right mouse button to zoom out. You can set the zooming percentage by selecting **Zoom Custom** from the **View** menu.

To zoom in on a selected area, click and hold the left mouse button while in zoom mode. When you hold the mouse button and drag in zoom mode, the Class Definition tool draws a rectangle to indicate the zoom area. When you have the rectangle positioned in an area of the viewport, release the mouse button to select the area for zooming.

To return to the diagram, click the **Select Tool** button .

## Attributes

Attributes specify the exact nature of the information within a class or relationship. **User Defined Attributes** are those defined and maintained by the Administrator, all aspects of these attributes can be modified, new attributes may be defined at any time and old attributes hidden away from further use.










ou can define any number of attributes for each class and relationship. In addition to these user-defined attributes, there are implicit predefined attributes referred to as system attributes..



**NOTE** There are two implicit attributes that represent who created a requirement. The "Initial Created by" attribute contains the name of the user who initially created a requirement, and is retained when the requirement is replaced by another user. The name of the user who replaced the requirement is stored in the "Created by" attribute.

## Attribute Types

The following sections describe the attribute types. If the attribute has a second tab specific to the attribute, its parameters are included in the description.

	Attribute Type	Description	Page
	Alphanumeric	A single line of text up to 1000 characters.	<a href="#">277</a>
	Date	A date, the format of which (including length, default, minimum, and maximum values) can be defined by the administrator.	<a href="#">278</a>
	File Attachment	Can hold one or several files to be accessed from RM Browser.	<a href="#">278</a>
	Group	Like a list attribute, but composed of a series of sub attributes. The choices available to the user <i>depend</i> upon the selections they made in the higher level, or parent, attributes within the group attribute.	<a href="#">279</a>
	List	A list of values configured by the administrator for user selection. A list attribute can be configured to display as check box(es) or radio buttons.	<a href="#">283</a>
	Lookup	A lookup attributes allows to select one or several values (depends on the configuration of that attribute) that reference the PUID attribute or title attribute of any class.	<a href="#">288</a>
<a href="#">1.2</a>	Numeric	Accepts only numeric values.	<a href="#">290</a>
	Text	A block of text up to 64Kb in size.	<a href="#">291</a>
	URL	Allows to specify one or several URLs.	<a href="#">291</a>
	User	A list of user names, which can be configured by group or individual user names.	<a href="#">292</a>

## Alphanumeric Attribute

An alphanumeric attribute represents one line of alphanumeric text, such as the title of an acceptance test. It can be up to 1000 characters in length.

**Figure 9-5. Alphanumeric Attribute Definition**

The alphanumeric attribute properties are described in the following table.

Property	Description
Minimum Value	A minimum value that can be associated with the attribute, if any. Dimensions RM performs a string comparison on the minimum and maximum values. For example, if you enter a minimum value of A and a maximum value of C, Dimensions RM will inform you that a value of D is out of range.
Maximum Value	A maximum value that can be associated with the attribute, if any. Dimensions RM performs a string comparison on the minimum and maximum values. For example, if you enter a minimum value of A and a maximum value of C, Dimensions RM will inform you that a value of D is out of range.
Default Value	A default value for initial instances of the attribute, if required.
Maximum Length	The maximum length of the value allowed for the attribute. The valid range is 1 to 1000 characters.
Display Length	The default number of characters to display for this attribute. The valid range is 1 to 1000 characters.
Case	Whether the attribute value should be upper case, lower case, or sentence (mixed) case.

## Date Attribute

A date attribute can have values that are based on user-defined formats. A date attribute, for example, could be used for test dates.

**Figure 9-6. Date Attribute Definition**

The date attribute properties are described in the following table.

Property	Description
Minimum Value	A minimum value that can be associated with the attribute, if any.
Maximum Value	A maximum value that can be associated with the attribute, if any.
Default Value	A default value for initial instances of the attribute, if required.
Current Date	If enabled, uses the current server date (and time if defined for the attribute) as a default value.
Maximum Length	The maximum length of the value allowed for the attribute. The valid range is 1 to 1000 characters.
Display Length	The default number of characters to display for this attribute. The valid range is 1 to 1000 characters.
Display Format	The date format. <b>NOTE:</b> The default date formats use the string "RRRR" to represent a four-digit year. This is preferable to using "YYYY" because when the year is entered as two digits, this format will correctly populate the century based on the rules described in <a href="#">"RRRR Date Format Elements"</a> on page 330.

## File Attachment Attribute

A file attachment attribute can hold a single file or multiple files that can be accessed through RM Browser. Add one or more file attachment attributes to the class to which the file or files will be attached. For example, you could add the file attachment attributes *Use*

*Cases*, *Customer Letter*, and *Business Justification* to the Marketing Requirements class. Users then use RM Browser to add, view, or download the file(s).

For more information about using RM Browser to view and manage file attachments, see the *Dimensions RM Browser User's Guide*.

The file attachment attribute properties of the **Attach Settings** tab are described in the following table.


Property	Description
<b>Allow multiple selections</b>	Whether the attribute can hold one or multiple files. <ul style="list-style-type: none"> <li>■ Enabled: The attribute can hold multiple files.</li> <li>■ Disabled: The attribute can hold a single file.</li> </ul>

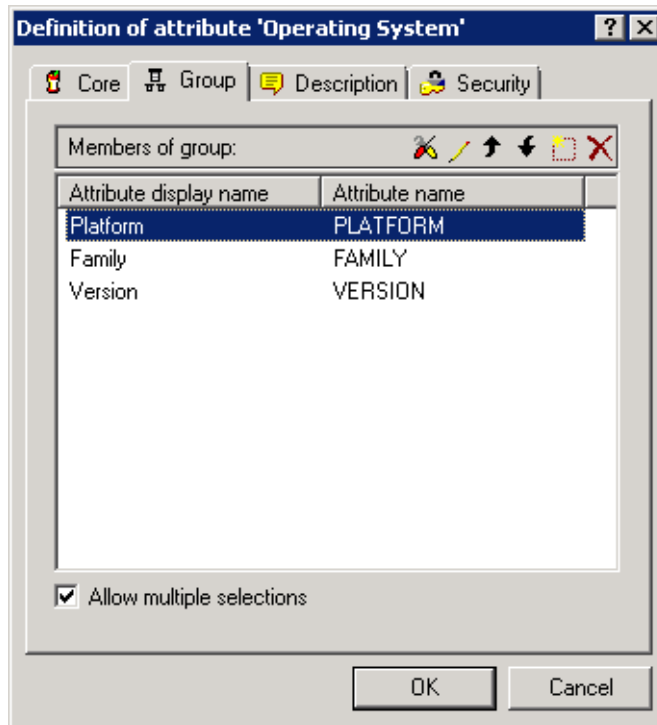
### **Group Attribute**


A group attribute allows to select values like a list attribute. But unlike a simple list attribute, a group attribute is composed of a series of sub-attributes. These sub-attributes are called **group members**. Each group member contains its own list of values which may be different depending on the selected value of the previous group member. For more details on how the group attribute works, see ["Explaining the Group Attribute" on page 282](#).



#### **Defining a group attribute:**


- 1 Allow multiple selections:** To allow users adding multiple rows, select this option. The default is cleared (Group attribute supports only one row).

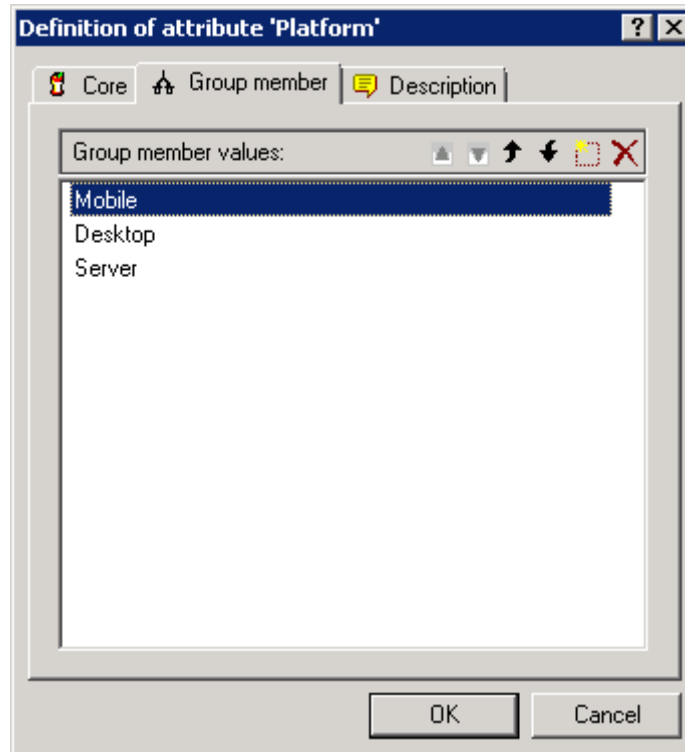
- To add members (sub attributes) to the group attribute, click the **New**  button (or press the **Insert** key) and enter a name. The name must be unique within the group attribute.









To delete a member attribute from the group, highlight the attribute and click the **Delete**  button, or press the **Delete** key.

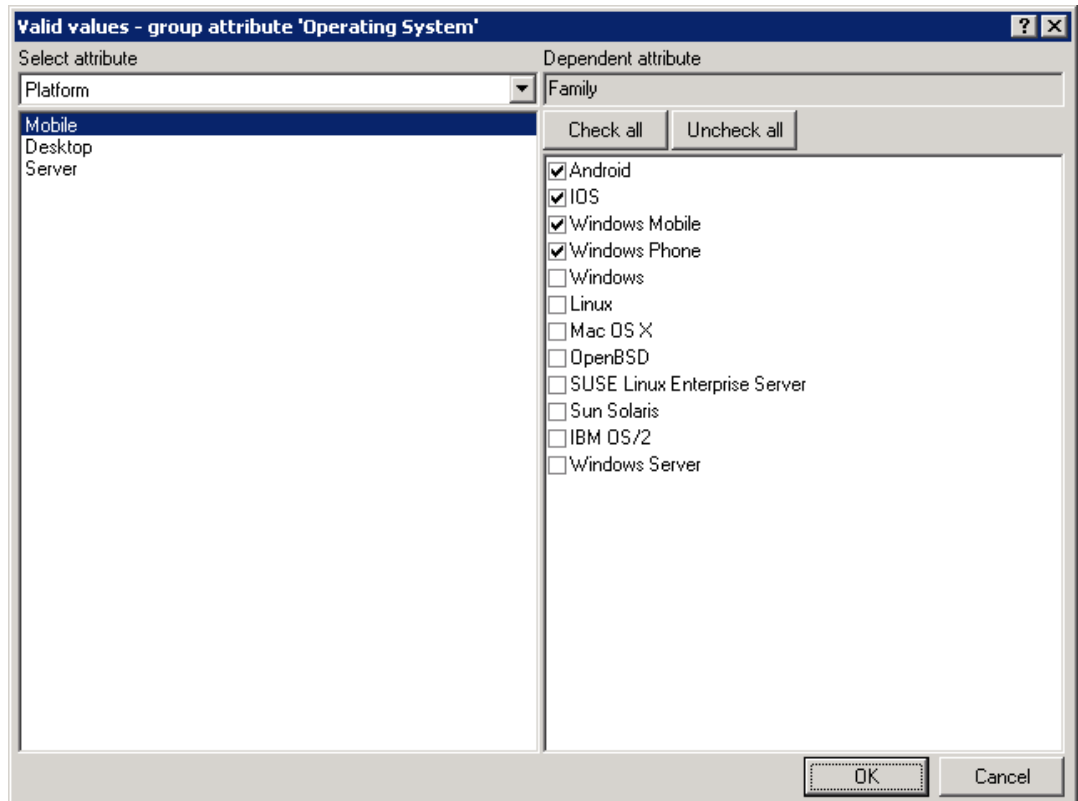
- The first attribute in the group is the parent of the second, and the second is the parent of the third, etc. To reorder the attribute members to reflect the dependency logic that you want to enforce, select the attribute you want to move and click the **Move Up**  or **Move Down**  button, or drag and drop the attribute to the desired position.

- 4 To define the values available for a member attribute, select the attribute and click the **Fields Options**  button. A Definition of attribute dialog opens for the group member (note the **Group member** tab).



- a To add values for a group member (sub attribute), click the **New**  button (or press the **Insert** key) and enter a name. The name must be unique within the group member.
- b The end user will see the values in the same order shown in this dialog. To reorder the list of values, do any of the following:
- To manually order the values, select a value and click the **Move Up**  or **Move Down**  button, or drag and drop the value to the desired position.
  - To alphanumerically sort the entire list of values, click the **Sort Ascending**  or **Sort Descending**  button.
- c Once you have defined and ordered the values for a group member, click the **OK** button to return to the Definition of attribute dialog for the group attribute (which has a **Group** tab rather than the **Group member** tab).
- 5 To define the dependencies between the values in a parent attribute and those in a child attribute, select a member attribute and click the **Edit value restrictions**  button. The Valid values dialog opens.

On the left is the list of values available for the selected group member. To the right is the name of the first-order child of the selected group member and the list of values available for that child attribute.



- a Select a member attribute from the **Select attribute** drop-down list.

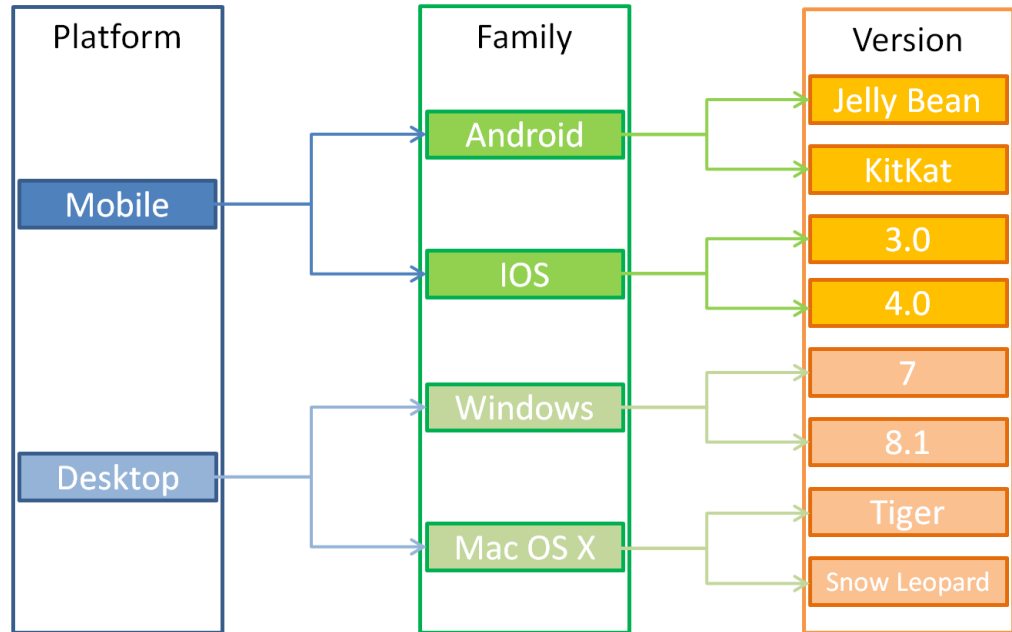


**TIP** Start with the topmost member attribute in the group and work your way in order through the child attributes.

- b In the left pane, select a value from the list available for the selected group member.
- c In the right (Dependent) pane, select the values to display for the child attribute whenever a user selects the value selected in [Step b](#) for the parent attribute.
- d Once you have defined the dependencies between member values, click the **OK** button to return to the Definition of attribute dialog for the group attribute.

### Explaining the Group Attribute

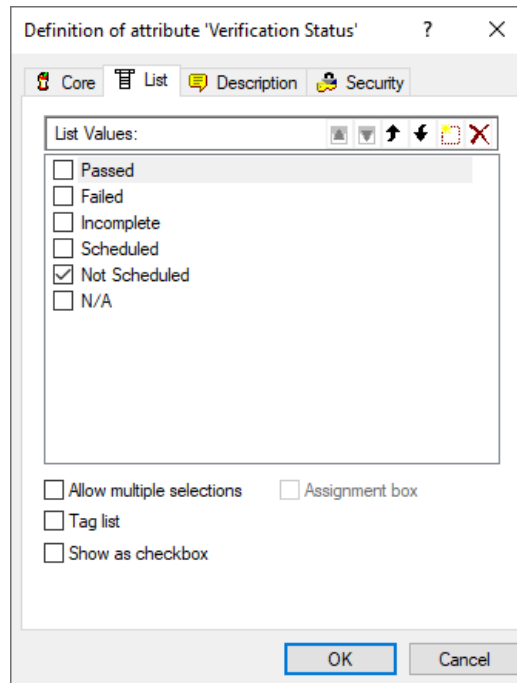
The following image shows a simplified representation of the group attribute **Operating System** of RMDEMO's **Tests** class.



The group attribute contains the group members **Platform**, **Family**, and **Version**. By restriction, you can define which values the user will see when selecting a value. The selection of the **Platform** group member defines the values of the **Family** group member. The selection of the **Family** defines the values of the **Version** group member.

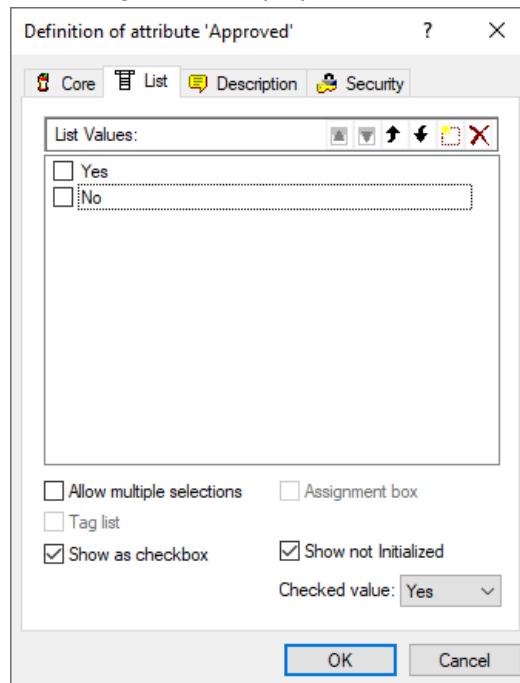
### **List Attribute**

A list attribute is a configurable attribute that provides a list of values for user selection. For example, you could define Passed, Failed, and Incomplete as the valid values for a list attribute Verification\_Status, and require that the user choose one or more of these values.






**Figure 9-7. List Attribute Definition**


A list attribute can also be configured to display as a checkbox or radio buttons.




**Figure 9-8. List Attribute Definition as Checkbox**

The list attribute properties are described in the following table.

Property	Description
<b>List Values</b>	A list of possible values that have been defined for the list attribute. A check in the box to the left of the value indicates this is a default value. Selecting the check box next to the desired attribute value can change the default value state.
<b>Allow multiple selections</b>	Whether the user can select one or more values from the list. If the box is not checked, you can select only a single value from the list.
<b>Assignment box</b>	Only available when <b>Allow multiple selections</b> is selected and <b>Tag list</b> is not selected. Enabling this option replaces a single list with two lists which allow adding/removing entries by using  and  .
<b>Tag list</b>	Attribute values are displayed as "tags". Enabling this option also means that each user having write access can add values to this attribute.   <b>CAUTION!</b> When saving the instance schema, all data the Class Definition tool loaded for that schema will be written. If users added tags during the time span the class schema was opened by the Class Definition tool, the users' values will be removed (as the Class Definition tool did not load them when opening the schema). It is <b>strongly</b> suggested to make changes to the class definition outside business hours.
<b>Show as checkbox</b>	The list attribute is displayed as checkbox or radio buttons. For further details, see chapter " <a href="#">Configuring a List Attribute</a> " on page 287.
<b>Show not Initialized</b>	Show the option <b>Not Initialized</b> for a radio button or the text <b>Not Initialized</b> for a checkbox. For further details, see chapter " <a href="#">Configuring a List Attribute</a> " on page 287.
<b>Checked value</b>	Specifies which list value will be used for the selected state of the checkbox.

To add a new value to the list of possible values click the  button (or press the **Insert** key) and enter a name to the list. The name for the value must be unique within the list.

To delete a value from the list, highlight the value by left-clicking it and either click the **Delete**  button or press the **Delete** key. The following operation depends on the status of the list value:

**List value has not been used in any requirement:**

The value is deleted immediately.

**List value has been used in a requirement:**

Opens the **Class Definition - Warning** dialog which offers 3 functions:

- **Delete:** Marks the attribute as deleted. This means:
  - The value is visible in requirements having this value, but it cannot be selected.

- The value is available in all dialogs which allow filtering or searching (e.g. Quick Search).
- **Remove:** Completely deletes the value from Dimensions RM database. This means:
  - With the **Edit Attributes** dialog, the attribute in a requirement which previously used this value is empty.
  - Any result list (e.g. Quick Search, reports) or a document showing a requirement which previously used this value will show the value for this attribute (if displayed).
  - The value is no longer available in any dialog.
- **Cancel:** Keeps the list value and returns to the **Definition of attribute 'Attribute Name'** dialog.

#### List value has been deleted:

- **Remove:** Completely deletes the value from Dimensions RM database. This means:
  - With the **Edit Attributes** dialog, the attribute in a requirement which previously used this value is empty.
  - Any result list (e.g. Quick Search, reports) or a document showing a requirement which previously used this value will show the value for this attribute (if displayed).
  - The value is no longer available in any dialog.
- **Cancel:** Keeps the list value and returns to the **Definition of attribute 'Attribute Name'** dialog.







#### **IMPORTANT!** Removing Existing List Values from the Schema:

- If you remove an existing list value from the instance schema:
  - It is no longer selectable for new entries, but it will continue to display in reports or Quick Search for any requirement versions where this value had already been set.
  - Any time a requirement that has that value is opened in the editor, the list will default to having no value. If the field is required, you will have to select a value.
- Deleting/Editing an existing list value in the instance schema changes the value available for selection going forward. It does not directly change the value stored in existing requirement versions. If you want to replace an old/obsolete value in requirement versions, see ["Changing a List Value on Existing Data" on page 287](#).

#### Ordering List Values

The end user will see the values in the same order shown in this dialog. To reorder the list of values, do any of the following:

- To manually order the values, select a value and click the **Move Up**  or **Move Down**  button, or drag and drop the value to the desired position.
- To alphanumerically sort the entire list of values, click the **Sort Ascending**  or **Sort Descending**  button.

## Changing a List Value on Existing Data

This section describes a suggested best practice for changing a list value that has been in use and thus exists in non-current requirement versions. It presupposes that you need to replace an obsolete list value in non-current versions and that an audit trail must be maintained.

- 1 Do a backup of the instance, including security.
- 2 Add the new list value to the instance schema. (Do not remove the old value.)
- 3 Ensure that you have both Update and Update Non-Current access to the class that includes the modified list.
- 4 Create a report that lists:
  - PUID
  - Object\_ID
  - The relevant list field with the obsolete value
- 5 Save the report as CSV.
- 6 Edit the CSV to change the obsolete value to the new value.
- 7 Add a **Reason for change** column and populate it with whatever statement satisfies your audit requirements. (This will overwrite existing **Reason for Change** entries.)
- 8 Use CSV Import in **Update** mode to match on Object\_DF and map the list and reason for change attributes.
- 9 Verify that the data was correctly imported.
- 10 Remove your Update and Update Non-Current access to the class (assuming you added these just for this procedure).
- 11 Remove the old list value from the instance schema.

## Configuring a List Attribute

Check boxes or radio buttons are configuration options for the list attribute. See chapter "[List Attribute](#)" on page 283 for more information on creating list attributes.

The configuration of a list attribute as check box(es) or radio buttons depends on the overall configuration of the list attribute and the options **Show as checkbox** and **Show not Initialized**. Note that **Show not Initialized** is not always available.

### Configuring a Yes-No Checkbox

A Yes-No checkbox has two values and does not show any additional text apart from its attribute name.

#### To create a Yes-No checkbox:

- 1 Create a list attribute and specify two values in the list, e.g. *Yes* and *No*.
- 2 Select the **Show as checkbox** option.
- 3 From the **Checked value** box, select the value you want to use with the selected state of the checkbox, e.g. *Yes*. The second list value (e.g. *No*) will automatically be used for the clear state of the checkbox.

- 4 Select the checkbox next to *Yes* or *No* to specify the default value for the attribute.
- 5 Click **OK**.

### **Configuring a Three-State Yes-No Checkbox**

A Yes-No checkbox has two values and does not show any additional text apart from its attribute name. A three-state checkbox provides an additional state, which is **Not Initialized**.

#### **To create a Yes-No checkbox:**

- 1 Create a list attribute and specify two values in the list, e.g. *Yes* and *No*.
- 2 Select the **Show as checkbox** option.
- 3 Select the **Show not Initialized** option.
- 4 From the **Checked value** box, select the value you want to use with the selected state of the checkbox, e.g. *Yes*. The second list value (e.g. *No*) will automatically be used for the clear state of the checkbox.
- 5 Click **OK**.

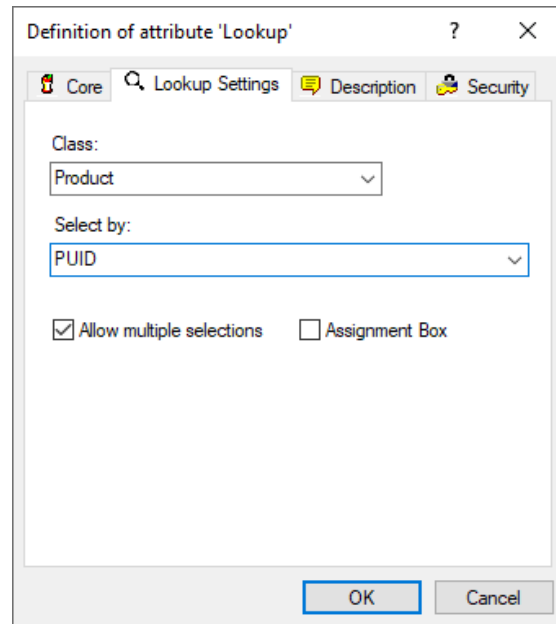
### **Configuring Multiple Checkboxes or Radio Buttons**

When a list has more than 2 values, the list will show either radio buttons or several checkboxes. If the list supports only single value selection, the list will show as radio buttons. For multiple selection, the list will show checkboxes.

- 1 Create a list attribute and specify three or more values in the list.
- 2 To allow selection of more than one value, select the **Allow multiple selections** option.
- 3 Select the **Show as checkbox** option.
- 4 If desired, select the **Show not Initialized** option.
- 5 Click **OK**.



### **Lookup Attribute**

A lookup attributes allows to select one or several values (depends on the configuration of that attribute) that reference the PUID attribute or title attribute of any class.



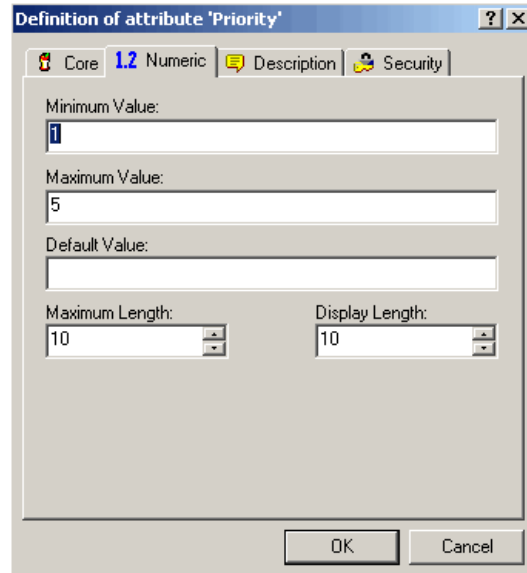
**Figure 9-9. Lookup Attribute Definition**

The properties are described in the following table:

Property	Description
<b>Class</b>	The class that relates to the current class.
<b>Select by</b>	The attribute that provides the values for the list.
<b>Allow multiple selections</b>	Whether the user can select one or more values from the list. If the box is not checked, you can select only a single value from the list.
<b>Assignment Box</b>	Only available when <b>Allow multiple selections</b> is selected. Enabling this option replaces a single list with two lists which allow adding/removing entries by using  and  .

## Numeric Attribute

A numeric attribute accepts only numeric values, such as a reference number. The value can include a decimal point.



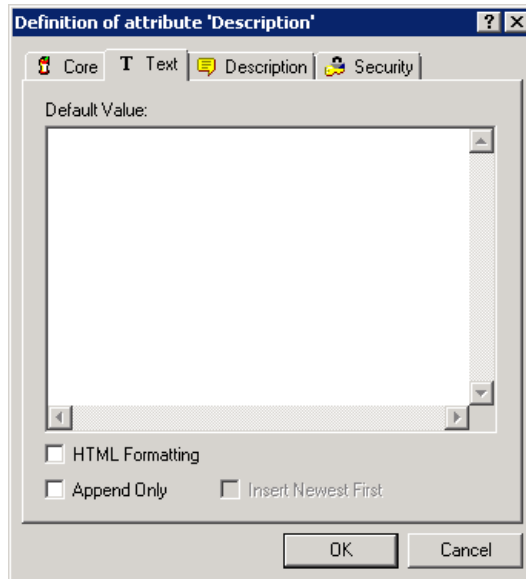
**Figure 9-10. Numeric Attribute Definition**

The numeric attribute properties are described in the following table.

Property	Description
Minimum Value	A minimum value that can be associated with the attribute, if any.
Maximum Value	A maximum value that can be associated with the attribute, if any.
Default Value	A default value for initial instances of the attribute, if required.
Maximum Length	The maximum length of the value allowed for the attribute. The valid range is 1 to 1000 characters.
Display Length	The default number of characters to display for this attribute. The valid range is 1 to 1000 characters.

## Text Attribute

A text attribute is a text block (up to 64Kb) that can span more than one line. It is suitable for long descriptions, such as the description of an acceptance test.



**Figure 9-11. Text Attribute Definition**

The text attribute properties are described in the following table.

Property	Description
Default Value	A default value for initial instances of the attribute, if required.
HTML Formatting	A check box that allows you to specify whether this text attribute is enabled for HTML formatting. When you edit an HTML-enabled text attribute in RM Browser, a special HTML edit control is displayed in place of the normal text area. <b>NOTE:</b> The HTML Formatting property cannot be disabled in the Chapter class.
Append Only	If enabled, the text the user enters into the text box does not replace the current text, but added to the current text. The history is shown above the associated text box.
Insert Newest First	If enabled, new text is placed before any existing text. If disabled, new text is placed after any existing text.

## URL Attribute

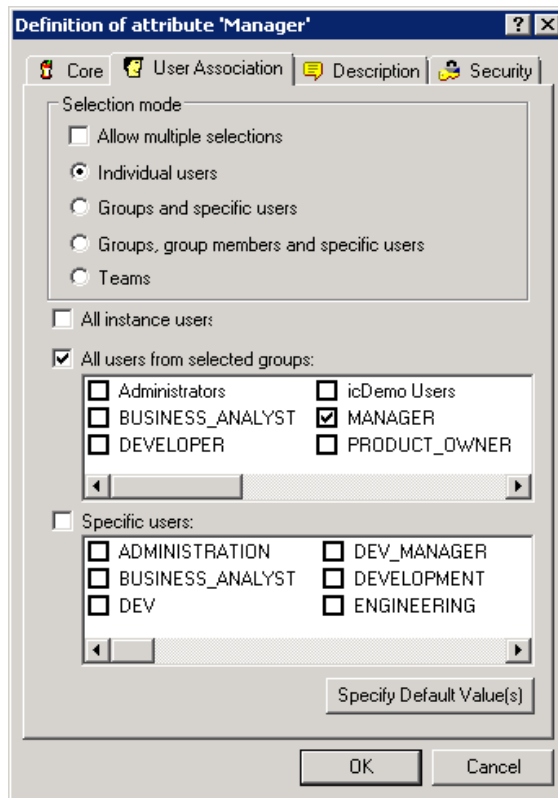
A user attribute can hold one or multiple URLs. Clicking the URL opens it in a new tab or window of your web browser.

The URL attribute supports the following settings:

Property	Description
Mode	<ul style="list-style-type: none"> <li>■ <b>Single:</b> The URL attribute can only hold one URL.</li> <li>■ <b>Multiple:</b> The URL attribute can hold several URLs.</li> </ul>
Limit count to	This option is only available if <b>Mode</b> is set to <b>Multiple</b> . Select this option and specify any value higher than 0 to define the maximum number of URLs the attribute can hold.
Validation pattern	<p>Specifying a validation pattern allows to ensure that URLs match a certain format. The validation pattern must be a regular expression for the JavaScript programming language. The following samples are provided in the drop-down list:</p> <ul style="list-style-type: none"> <li>■ <code>^(http[s]? ftp):\/\/(.*)</code> The URL must use either the HTTP, HTTPS or FTP protocol.</li> <li>■ <code>^https:\/\//www\.opentext\.com\/(.*)</code> The URL must use the HTTPS protocol and the server must be www.opentext.com.</li> </ul>
Placeholder	Specify a text to inform users about the expected format.

### **User Attribute**

A user attribute is a configurable attribute that provides a list of user names for user selection. It can store one single value and can be configured to list all users, all members of one or several groups or individual users.



**Figure 9-12. User Attribute Definition**

**To list all users, follow these steps:**

- 1 Select option **All instance users**.
- 2 Click **OK**.

**To list users of one or several groups, follow these steps:**

- 1 Select option **All users from selected groups**.
- 2 Select the groups you want to be included in the list.
- 3 Click **OK**.

**To list individual users, follow these steps:**

- 1 Select option **Specific users**.
- 2 Select the users you want to be included in the list.
- 3 Click **OK**.

**Selection Mode**

Property	Description
Allow multiple selections	If selected, allows multi-selection. If cleared, allows single selection.
Individual users	Only users can be selected.

Property	Description
Groups and specific users	Groups selected in the <b>All users from selected groups list</b> and users specified in the <b>Specific users</b> list can be selected.
Groups, group members and specific users	Groups selected in the <b>All users from selected groups list</b> , users who are members of the selected groups and users specified in the <b>Specific users</b> list can be selected.
Teams	Only teams can be selected.

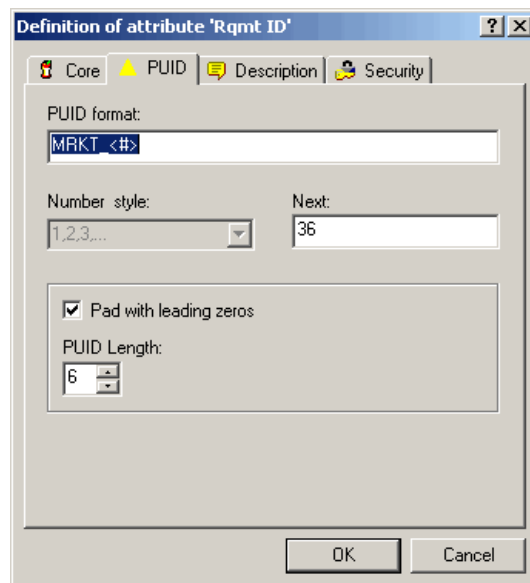
### Specifying Default Values

To specify a group or user as a default value, do the following:

- 1 Click the button Specify Default Value(s). This opens the **Specify Default Value** dialog.
- 2 Select the user or group you want to use as a default value. The **<Current User>** entry uses the name of the user who edits the requirement as a default value.
- 3 Click **OK**. Note that the default value is not used until you save the class definition.

### Rqmt ID Attribute

The Rqmt ID implicit attribute represents the PUID of a requirement. The PUID is a unique identifier that does not change. *There is no button associated with this attribute, because it is automatically included in every class.*



**Figure 9-13. Rqmt ID Attribute Definition**

The Rqmt ID attribute properties are described in the following table.

Property	Description
PUID format	Any string of characters and then <#>. The <#> variable is replaced by the PUID number. <b>NOTE:</b> If you want # to appear in the PUID as a character, type it in the string of characters without the brackets.
Number style	The style of numbering to use for the PUID.
Next	The next PUID number to be assigned.
PUID Length	The number of numbers that can replace the <#> variable.
Pad with leading zeros	Adding padding to the PUID number ensures consistency in display, as well as the ability to use filters such as greater-than, less-than, and between when filtering a list. The default padding is 5, which means that a Functional Requirement (prefix FR) will extend the initial ID to a length of 5: FR_00001.  The length of the PUID padding later in the life of the class.

## Adding an Attribute

**To add a new attribute to a class or relationship definition:**

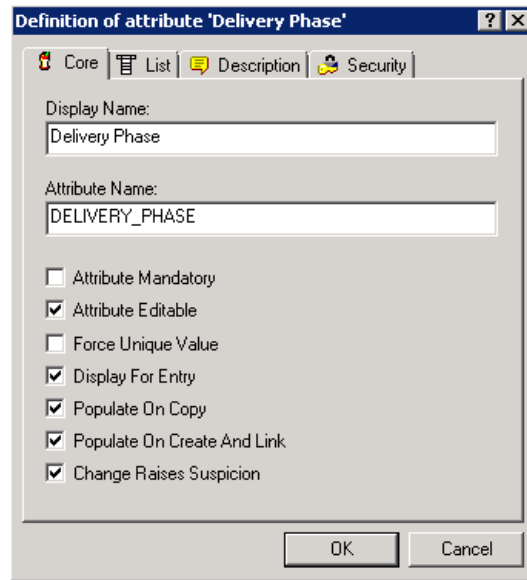
- 1 In **Class Definition**, do one of the following to open the **Definition of class** or **Definition of relationship** dialog box:
  - Double-click the desired class or relationship.
  - Right-click the desired class or relationship and select **Define**.
- 2 To add the attribute to the class or relationship definition, click the appropriate button at the left of the panel for the user-defined attribute type you want to add. For further information about attribute types, see chapter "[Attribute Types](#)" on page 276.
- 3 Click **OK**.

## Defining an Attribute

**To define an attribute:**

- In **Class Definition**, double-click the attribute in the tree control, or highlight it and press **Enter**.

The **Definition of attribute** dialog box opens.



**Figure 9-14. Attribute Definition**

### Core Tab

The **Core** tab is displayed for all attribute types and is used to define attribute properties that are common to all attribute types. The core attribute properties are defined in the following table.

Property	Description
Display Name	The name of the attribute that will be displayed by the other Dimensions RM tools. Please consider the naming restrictions when specifying the display name. For details about naming restrictions, see chapter " <a href="#">Naming Conventions for Attribute Display Names</a> " on page 28.
Attribute Name	The internal name of the attribute, which is populated automatically for a new attribute based on the display name if no value is provided. Please consider the naming restrictions when specifying the attribute name. For details about naming restrictions, see chapter " <a href="#">Naming Conventions for Attribute Names</a> " on page 29.
Attribute Mandatory	Whether you are required to specify values for the attribute during the information storage or capture process.
Attribute Editable	Whether you can edit the attribute values. Conversely, making an attribute non-editable is useful when no further changes to the attribute are allowed.
Force Unique Value	Whether you must enter a unique value for an instance of this attribute (no duplicate values are allowed). This may be grayed out.
Display For Entry	Whether the attribute will be displayed in forms and list views of object content. If unchecked, the attribute will not be presented in these views. This is generally unchecked when retiring an attribute or for reasons of security.

Property	Description
Populate on Copy	<p>Whether the attribute will be pre-populated when you copy a requirement. To prevent the situation where duplicate requirements are created by mistake, it is a good practice <i>not</i> to copy the Title and Description attributes.</p> <p>When using <b>Populate on Copy</b> with a container workflow and the container workflow is assigned to a document, the attribute value will be copied to the new document if this option is enabled.</p>
Populate on Create and Link	<p>The attribute will be pre-populated when you create a requirement and link to it. This only applies to relationships where the "populate attributes on create and link" setting is enabled (see chapter "<a href="#">Transfer Rules</a>" on page 312).</p>
Change Raises Suspicion	<p>This setting is available for any custom attribute and the following system attributes:</p> <ul style="list-style-type: none"> <li>■ <b>Category:</b> The <b>Category</b> attribute changes when a requirement is moved to a different category.</li> <li>■ <b>Class ID:</b> The <b>Class ID</b> attribute changes, when a requirement is changed to a different class (e.g. <i>Marketing_Requirements</i> to <i>Product_Requirements</i>).</li> <li>■ <b>Owner:</b> The <b>Owner</b> attribute of a requirement can be changed by a workflow transition</li> <li>■ <b>Workflow State:</b> The <b>Workflow State</b> attribute changes when a requirement is transitioned to a different state.</li> </ul> <p>If this setting is enabled, any replace action on this attribute will mark linked objects as <b>Suspect</b> if this is enabled in the relationship definition (see chapter "<a href="#">Transfer Rules</a>" on page 312).</p>

### Attribute Type Tab

The second tab is specific to the attribute type selected in [Step 2 on page 295](#). The attribute type tabs are described under "[Attribute Types](#)" on page 276.

### Description Tab

The **Description** tab is used to add a description to the attribute.

### Security Tab

The **Security** tab allows a security profile to be created for the attribute. For information about entering properties on the **Security** tab, see "[Security](#)" on page 320.



**NOTE** You can edit an attribute definition at any time after having defined it. This could mean that values of the attribute become invalid for certain instances of the class. For example, if a Force Unique Value property is added to an attribute, existing non-unique values must be changed prior to replacement.

## Retiring an Attribute


There are times, as processes evolve, that attributes may be deemed no longer useful. Such attributes may be deleted, but the more reasonable option, especially if the attribute has been gathering information for months or years, is to hide it from view.

By unchecking all boxes in the **Core** tab (see "Core Tab" on page 296), the attribute will disappear from view.

If the attribute has been specifically included on forms, it should be removed.

## Deleting an Attribute

To delete an attribute from a class or relationship:

- 1 In Class Definition, do one of the following:
  - Double-click the desired class or relationship.
  - Right-click the desired class or relationship and select **Define**. The **Attribute Definition** dialog box opens.
- 2 Select the attribute you want to delete from the definition.
- 3 Click the **Delete** button  or press the **Delete** key.
- 4 Click **OK**.



**NOTE** Implicit attributes cannot be deleted from the class or relationship definition.

## Classes

Classes act as repositories for the data held in the instance. Creating classes involves configuring the attributes of the class to tailor the class for the instance-unique

information that it will hold, as well as setting up the security profiles for individual groups and users to each of the classes.



### CAUTION!

- The Poll class is for internal use only and must not be modified.
- The Chapter class is for internal use only.

You **must not** modify or rename any of the following attributes:

- Chapter Description
- Chapter Type
- CM Associations short
- Doc Description
- Hide Chapter Number
- Reasons for Change
- Title

You may

- add attributes;
- show or hide the **Hide Chapter Number** attribute.

- The Comment class is for internal use only.

You **must not** modify or rename any of the following attributes:


- Comment
- Subject

You may add attributes.

## Adding a New Class

Adding a class symbol to the Class Definition diagram creates an information class.

### To add a class:

- 1 In **Class Definition**, click the **Add Class** button , or right-click a blank area of the canvas and select a class from the context menu.
- 2 Move the cursor to where you want to place the class and click the left mouse button. The class symbol is displayed on the diagram and the title is highlighted for editing.
- 3 Enter a unique name for the class that describes the data held in the class.



**CAUTION!** The class name must follow the conventions specified in chapter ["Naming Conventions for Class Names"](#) on page 28.

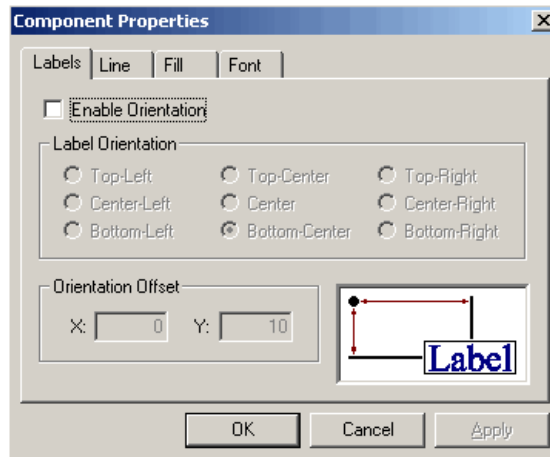
- 4 Click a blank area of the canvas to save the new name.

## Changing Display Properties for a Class

When a class is added to the instance schema, it is added with a default set of properties that relate to the graphic representation used for the class.

### To configure the display properties for a class:

- Right-click the class and select **Properties**. The **Component Properties** dialog box opens.



**Figure 9-15. Component Properties**

The **Component Properties** dialog box consists of four tabs:

- Labels**—Allows the location of the label to be specified. The **X Offset** and **Y Offset** fields allow the offset of the label to be specified relative to the selected control point. To reposition a class label relative to the bitmap, use the X and Y Offset values rather than dragging the label to its new location. This leaves the label attached to the bitmap so that it will move when the class bitmap is moved. If the label is repositioned by dragging it on the canvas, it will not move when the class bitmap is moved. To reattach the label, select one of the control points and click **OK** or **Apply**.
- Line**—Allows the outline for the label to be defined. By default the line is not visible but it can be displayed by clearing the **Transparent** check box.
- Fill**—Allows the background fill for the class label to be defined. The default is transparent.
- Font**—Allows the font for the class label to be defined. The font, size, style and color can all be configured on this page.

## Changing a Class Image

When a class is added to the instance schema it is created with the default image associated with the type definition. The image for a class can be customized to uniquely identify a class on the diagram.

**To change the image for a class:**

- 1 Obtain or prepare an image file to be used for the class.



**NOTE** Class Definition only allows bitmaps of up to 8-bit color.

- 2 In **Class Definition**, right-click the class and select **Change Image**.
- 3 Locate the image file to be used for the class. The image bitmap is displayed in the preview area of the dialog. Bitmaps are the only file types allowed for this procedure.
- 4 Click **Open**.

## Copying a Class

You can copy a class definition to create a duplicate class definition on the instance schema diagram. The duplicate class must have a unique name, but will initially contain the same attributes as the original class.

**To copy a class:**

- 1 In **Class Definition**, select the class.
- 2 Right-click the class and select **Copy**.
- 3 Right-click the canvas where the class is to be displayed and select **Paste**.



**NOTE** This does not copy the data associated with the class.

## Creating a Class Type from a Class

Class types provide a way to reuse all or part of a class definition within an instance schema. You can define a class type from an existing class definition. The class type serves as a template for new class information.

**To create a new class type from an existing class instance:**

- 1 In **Class Definition**, right-click the class.
- 2 Select **Create as Class Type**. This creates a new class type with the same name as the existing class.
- 3 Modify the new class type in the **Definition of Class Type** dialog box (see ["Defining a Class" on page 302](#)).

## Deleting a Class

**To delete a class from the instance schema:**

- 1 In **Class Definition**, right-click the class you want to delete.

- 2 Select **Delete**, or select the class and then press the **Delete** key.



**NOTE** This will not only delete the class definition from the instance schema, but will also delete all data associated with the class. Therefore, use this procedure with caution.

## Purging Class Data

**To purge the data from a class:**

- 1 In **Class Definition**, right-click the class and select **Purge** from the shortcut menu.
- 2 Click **Yes** to purge the objects of the selected class.



**CAUTION!** Purging removes all objects from the selected class permanently. Purged objects cannot be restored.

## Renaming a Class

**To rename a class:**

- 1 In **Class Definition**, position the cursor over the class title.
- 2 To select the text, double-click the class title.
- 3 Type a new name for the class.



**CAUTION!** The class name must follow the conventions specified in chapter "[Naming Conventions for Class Names](#)" on page 28.

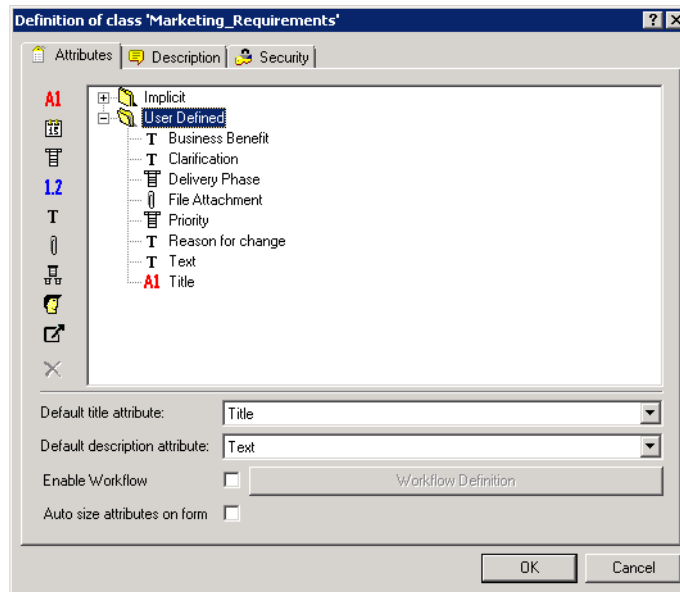
- 4 To commit the name change, click an empty area of the canvas.

## Defining a Class

**To define a class:**

- 1 Select a class on the Class Definition diagram.

- 2 Right-click and select **Define**. The **Definition of Class** dialog box opens.



**Figure 9-16. Class Definition**

The **Definition of Class** dialog offers these functions:

Function	Description
Attributes tab	Allows management of attributes of the class. For details, see chapter <a href="#">"Attributes" on page 275</a> .
Description tab	Allows to set a description to the class.
Security tab	Allows to create security profiles for the class. For details, see chapter <a href="#">"Security" on page 320</a> .
Default title attribute	Allows to select the attribute which is used as a title. Only alphanumeric attributes can be selected. For details, see chapter <a href="#">"Alphanumeric Attribute" on page 277</a> .
Default description attribute	Allows to select the attribute which is used for the description. Only text attributes can be selected. For details, see chapter <a href="#">"Text Attribute" on page 291</a> .
Enable Workflow	If enabled, the class is using a workflow for each requirement.
Workflow Definition	Opens the Workflow Definition editor. For details, see chapter <a href="#">"Workflows" on page 331</a> .
Auto size attributes on form	If enabled, all attributes have the same width on forms.

### Class Definition for ReqIF

When importing ReqIF files frequently, you can use auto-selection on ReqIF import. For auto-selection it is required that you create class attributes according to this schema:

Type	Display Name	Attribute Name	Length
Alphanumeric	<Custom>	DOORS_ID	length of the longest possible value
Alphanumeric	<Custom>	REQIF_ID	length of the longest possible value
Alphanumeric	<Custom>	REQIF_OWNER	length of the longest possible value
File Attachment	<Custom>	ATTACHMENT	N/A

For detailed information about defining attributes, see chapter ["Attributes" on page 275](#).

## Specifying Attributes

Each class has to have the following:

- A default title attribute
- A default description attribute

In RM Browser, Documents View uses the default title attribute and default description attribute to display meaningful data. Only the title for each chapter and requirement is displayed in the navigation tree. In the paragraph layout, the title, description, and any additional attributes that were selected in the **Properties** dialog box are displayed.

The default title attribute and default description attribute are also displayed in the prebuilt queries in Home View, in the query results from running a quick search from Requirement View, and in the detail pane for a selected requirement in Traceability View.

For more information about these views, see the *Dimensions RM Browser User's Guide*.

#### To specify values on the Attributes tab:

- 1 In the **Default title attribute** list, select an attribute. All alphanumeric attributes that are defined for the class are listed. You must set the default title attribute to an existing alphanumeric attribute or create a new alphanumeric attribute if none is available.
- 2 In the **Default description attribute** list, select an attribute. All text attributes that are defined for the class are listed. You must set the default description attribute to an existing text attribute or create a new text attribute if none is available.



**NOTE** For information about defining individual attributes, see ["Attributes" on page 275](#).

## Specifying a Description

The Class Definition tool allows a description to be associated with all items defined in the instance schema. Use this field to clarify items. For example, an attribute, "Build Version" might have the description "Enter the build version in which the feature was released."

- 1 In **Class Definition**, double-click the class. The **Definition of class** dialog box opens.
- 2 Click the **Description** tab.
- 3 Type the description.

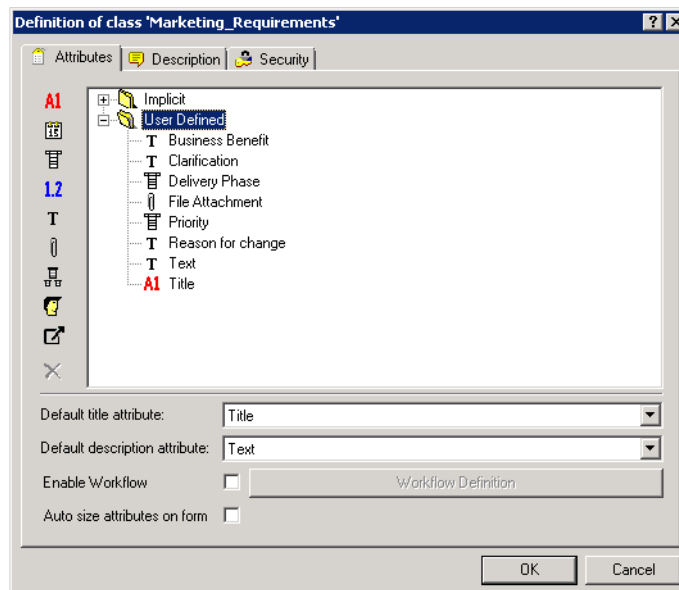
## Specifying Security

For information about specifying security, see ["Security" on page 320](#).

## Specifying Equal Control Width on Forms

The **Auto size attributes on form** option ensures that all attribute controls use an equal width.

- 1 Select a class on the Class Definition diagram.
- 2 Right-click and select **Define**. The **Definition of Class** dialog box opens.



**Figure 9-17. Class Definition**


- 3 Select **Auto Size attributes on form**.
- 4 Click **OK** to close the **Definition of Class** dialog and confirm your setting.
- 5 Save the instance schema.

# Relationships

A relationship represents a logical association between two classes. The two classes are referred to as the primary class (the class from which the relationship flows), and the secondary class (the class to which the relationship flows).

## Adding a New Relationship

Adding a relationship to the Class Definition diagram creates a link between two classes allowing the traceability or flow of information to be created between objects of the classes. A relationship can be created in one of three ways:

- Click the **Add Relationship** button  and move the cursor over one of the classes to be linked. Click the left mouse button to start the relationship and then trace the route of the relationship by moving the mouse and clicking the left mouse button to create a vertex. Finally, click on the destination class with the left mouse button to complete the relationship.
- Right-click a blank area of the canvas and select **Add Relationship**. Move the cursor over one of the classes to be linked. Click the left mouse button to start the relationship and then trace the route of the relationship by moving the mouse and clicking the left mouse button to create a vertex. Finally, click the destination class with the left mouse button to complete the relationship.
- Move the cursor over one of the classes to be linked and press the left mouse button while holding down the control key. Trace the route of the relationship by moving the mouse and clicking the left mouse button to create a vertex. Finally, click on the destination class with the left mouse button to complete the relationship.

The relationship will appear on the diagram and the name will be highlighted. Enter a unique name for the relationship which describes the data which will be held in the relationship, and click on a blank area of the canvas to commit the new name.



**CAUTION!** The relationship name must follow the conventions specified in chapter "[Naming Conventions for Relationship Names](#)" on page 29.



### NOTES

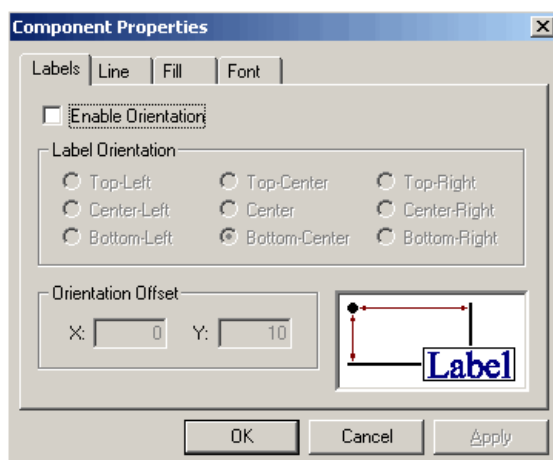
- Do not create a relationship from any class to a Chapter class.
- You cannot put more than one Chapter class into a diagram.

## Changing the Display Properties for a Relationship

When a relationship is added to the instance schema, it is added with a default set of properties that relate to the label style used for the relationship.

### To configure the display properties for the relationship label:

- 1 In **Class Definition**, right-click the relationship and select **Properties**. The **Component Properties** dialog box opens.



**Figure 9-18. Component Properties**

The **Component Properties** dialog box consists of four tabs.

- **Labels**—Allows the location of the label, relative to the bitmap, to be specified. The X Offset and Y Offset fields allow the offset of the label to be specified relative to the selected control point. In order to reposition a relationship's label relative to the bitmap, you should use the X and Y Offset values instead of dragging the label to its new location. This will still leave the label attached to the bitmap so that it will move when the relationship's bitmap is moved. If the label is repositioned by dragging it on the canvas it will no longer move when the relationship's bitmap is moved. To reattach the label, select one of the control points above and click **OK** or **Apply**.
  - **Line**—Allows the definition of the outline for the label to be defined. By default the line is transparent (that is, not visible) but it can be displayed by clearing the **Transparent** check box.
  - **Fill**—Allows the background fill for the relationship's label to be defined. Once again the default is for a transparent background.
  - **Font**—Allows the font used for the relationship's label to be defined. The font, size, style and color can all be configured on this page.
- 2 Specify properties.
  - 3 Click **OK**.

## Deleting a Relationship

Deleting a relationship not only deletes the relationship definition from the instance schema. It also deletes all links associated with the relationship and should be used with caution.

### To delete a relationship from the instance schema:


- 1 In **Class Definition**, right-click the desired relationship.
- 2 Either select **Delete** from the context menu or press the Delete key.

## Editing Vertices

When a relationship is selected, Class Definition places control handles on every vertex that defines the relationships shape. These vertices can be manipulated to change the path of a relationship.


### ***Moving a Vertex***

#### **To move a vertex:**

- 1 In **Class Definition**, select the relationship.
- 2 Hover your cursor over a control handle. The cursor changes  to signal that you can move this vertex.
- 3 Click the control handle and then drag it to a new position.
- 4 Release the mouse button to place the vertex at its new coordinates.


### ***Inserting a Vertex***

#### **To insert a vertex:**

- 1 In **Class Definition**, select the relationship.
- 2 Move your cursor between two control points and hold down the Control key. The cursor changes  to signal that you can insert a vertex.
- 3 Click to place the vertex on the line segment.

### ***Removing a Vertex***

#### **To remove a vertex:**

- 1 In **Class Definition**, select the relationship.
- 2 Move your cursor over a vertex and hold down the Control key. The cursor changes  to signal that you can delete the vertex.
- 3 Click to delete the vertex from the component.

## Purging Relationship Data

#### **To purge the links from a relationship:**

- 1 In **Class Definition**, right-click the relationship and select **Purge** from the shortcut menu.
- 2 Click **Yes** to purge the links of the selected relationship.



**CAUTION!** Purging removes all links of the selected relationship permanently. Purged links cannot be restored.

## Renaming a Relationship

The relationship name should describe the data you intend to associate with the relationship. Each relationship name must be unique to the diagram.



**CAUTION!** The relationship name must follow the conventions specified in chapter "Naming Conventions for Relationship Names" on page 29.

### To rename a relationship:

- In **Class Definition**, double-click the relationship name.

### To commit the name change:

- In **Class Definition**, click on a blank area of the canvas.

## Reversing a Relationship

If the information does not seem to flow in the direction that the relationship was initially created, you can reverse it.

### To reverse a relationship:

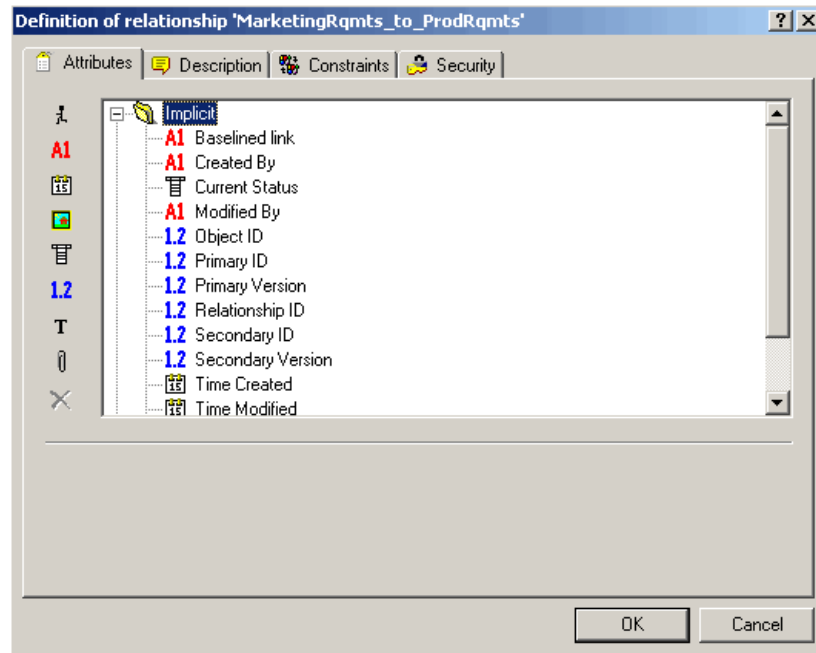
- 1 In **Class Definition**, right-click the relationship and select **Reverse**.
- 2 Select one of the following options. The selected option is applied to all existing links when the relationship is reversed.
  - **Retain Links**—Reverses the direction of the relationship while leaving all existing links in place.
  - **Remove Links**—Reverses the direction of the relationship, and removes all existing links for the relationship.

## Defining a Relationship

### To define a relationship:

- In **Class Definition**, right-click the relationship and select **Define**.

The **Definition of relationship** dialog box opens.



**Figure 9-19. Relationship Definition**

This dialog box has four tabs:

- **Attributes**—Used to manage the attributes of the relationship
- **Description**—Used to add a description to the relationship
- **Constraints**—Used to add constraints to the relationship
- **Security**—Used to create security profiles for the relationship

## Specifying Attributes

For information about specifying attributes, see ["Attributes" on page 275](#).

## Specifying a Description

The Class Definition tool lets you describe all items defined in the instance schema. Use descriptions to clarify a particular item. For example, an attribute or build version may have a description of "Enter the build version in which the version was released."

- 1 In **Class Definition**, right-click the object and select **Define**.
- 2 The **Definition of relationship** dialog box opens.
- 3 Click the **Description** tab.
- 4 Type the description.

## Specifying Constraints

Relationship rules enable you to specify the properties of a relationship. You can constrain the creation of links by the user, and also specify the actions to be performed when either the primary or secondary objects participating in an AND or OR relationship are edited.

### To add constraints to a relationship:

- 1 In **Class Definition**, right-click the relationship and select **Define**.  
The **Definition of relationship** dialog box opens.
- 2 Click the **Constraints** tab.

Definition of relationship 'ProdRqmts\_Verified\_By\_Tests' ? X

Attributes Description Constraints Security

Primary Cardinality: n Secondary Cardinality: n

Primary Links:

- transfer to child
- delete from parent
- transfer to parent on deletion of child
- mark secondary as suspect on change
- mark secondary as suspect on link deletion
- mark secondary as suspect on removal from container
- populate attributes on create and link
- apply only for current version

Secondary Links:

- transfer to child
- delete from parent
- transfer to parent on deletion of child
- mark primary as suspect on change
- mark primary as suspect on link deletion
- mark primary as suspect on removal from container
- populate attributes on create and link
- apply only for current version

Attribute Constraints:  OR  AND

Class	Attribute	Constraint	Value

apply on link creation only  apply on link creation only

**Figure 9-20. Definition of Relationship—Constraints Tab**

- 3 Specify the constraints as described in the following sections.
- 4 Click **OK**.

### Cardinality

Cardinality rules control the number of links that you can make between objects of the classes in a relationship. For example, a cardinality of 2:3 (2 for the primary cardinality and 3 for the secondary cardinality) means that no more than two links can be made from an object of the primary class to objects of the secondary class. Also, no more than three links can be made from an object of the secondary class to objects of the primary class. To indicate that links cannot be made to objects of either the primary or secondary class, enter a value of 0 in the appropriate field. To indicate that the number of links created to objects of the either the primary or secondary class should be unconstrained, enter a value of **n** in the appropriate field.

See also option "apply only for current version" in section ["Transfer Rules" on page 312](#).

## Transfer Rules

Transfer rules govern what happens to an object link if you edit an object participating in the relationship. Toggling the desired values on or off sets the link transfer rules.

The following table describes the types of link transfer rules.

### Primary Links:

Rule Type	Description
transfer to child	When the primary object in the relationship is edited and replaced, the links from the primary object are copied to the new version.
delete from parent	When the primary object in the relationship is edited and replaced, the links from the previous version of the primary object are deleted.
transfer to parent on deletion of child	If the primary object is removed, the links are transferred to the previous version of that object.
mark secondary as suspect on change	When the primary object is modified, the secondary object is marked as suspect. To define the attributes that trigger a change see attribute setting <b>Change Raises Suspicion</b> in chapter <a href="#">"Core Tab" on page 296</a> .
mark secondary as suspect on link deletion or undeletion	When the link between the primary object and the secondary object is deleted, or undeleted, the secondary object is marked as a suspect.
mark secondary as suspect on removal from container	When the primary object is removed from a container (i.e. collection, document), the secondary object is marked as a suspect.
populate attributes on create and link	When the secondary object creates a new primary object and links to it, attribute values are copied from the secondary object to the primary object if the attribute names (not the display names) match. This setting only applies for those attributes which have the "Populate on Create and Link" setting enabled (see chapter <a href="#">"Core Tab" on page 296</a> ).
apply only for current version	This option is related to Cardinality and just comes into effect if the primary Cardinality has a numeric value. If it is enabled, only primary objects with status <b>Current</b> are considered. If it is disabled, all versions of the primary object are considered.
apply on link creation only	The attribute constraints are only evaluated when creating a new link on the primary object. If a link is transferred (copied to a new version of an object), the attribute constraints are ignored.

**Secondary Links:**

Rule Type	Description
transfer to child	When the secondary object in the relationship is edited and replaced, the links from the secondary object are copied to the new version.
delete from parent	When the secondary object in the relationship is edited and replaced, the links from the previous version of the secondary object are deleted.
transfer to parent on deletion of child	If the primary object is removed, the links are transferred to the previous version of that object.
mark primary as suspect on change	When the secondary object is modified, the primary object is marked as suspect. To define the attributes that trigger a change see attribute setting <b>Change Raises Suspicion</b> in chapter "Core Tab" on page 296.
mark primary as suspect on link deletion	When the link between the primary object and the secondary object is deleted, the primary object is marked as a suspect.
mark primary as suspect on removal from container	When the secondary object is removed from a container (i.e. collection, document), the primary object is marked as a suspect.
populate attributes on create and link	When the primary object creates a new secondary object and links to it, attribute values are copied from the primary object to the secondary object if the attribute names (not the display names) match. This setting only applies for those attributes which have the "Populate on Create and Link" setting enabled (see chapter "Core Tab" on page 296).
apply only for current version	This option is related to Cardinality and just comes into effect if the secondary Cardinality has a numeric value. If it is enabled, only secondary objects with status <b>Current</b> are considered. If it is disabled, all versions of the secondary object are considered.
apply on link creation only	The attribute constraints are only evaluated when creating a new link on the secondary object. If a link is transferred (copied to a new version of an object), the attribute constraints are ignored.

**Constraints**

Relationship constraints allow rules to be created that govern the creation of links between objects of the primary and secondary class. Constraints define when a link is created.



**IMPORTANT!** Starting with RM 12.8, constraints define when a link is created. Previous versions defined when **not** to create a link. Existing constraints will be converted during upgrade.

**To add a new constraint:**

- 1 Click **OR** or **AND** in the **Attribute Constraints** area to specify the type of logical relationship you are about to specify.

**NOTE**

- **OR:** If one of the constraints matches, the link will be created.
- **AND:** If all of the constraints match, the link will be created.

- 2 Click the **New Constraint** button  in the **Attribute Constraints** area.

A new row is added to the table and the **Class** and **Attribute** cells are populated based on the relationship you selected previously. If needed, click on these cells to select different values from a drop-down menu.

- 3 Click in the **Constraint** cell and select the desired constraint type from the drop-down menu. The following constraint types are available:

- **=** The attribute *exactly* equals the value.
- **!=** The attribute does **not** equal the value.
- **Like** The attribute includes the value as part of a larger string. When using **Like**, you would include one or more asterisks (\*) as wild cards to indicate where the value fits into the larger attribute string.

Examples:

- \*UNIX would **include** any value ending with UNIX, e.g. HP-UNIX
- \*UNIX\* would **include** any value that contains UNIX, e.g. HP-UNIX, HP-UNIX-11, UNIX-11
- UNIX\* would **include** any value starting with UNIX, e.g. UNIX-11
- **Not Like** The attribute **must not** include the value as part of a larger string. When using **Not Like**, you would include one or more asterisks (\*) as wild cards to indicate where the value fits into the larger attribute string.

Examples:

- \*UNIX would **exclude** any value ending with UNIX, e.g. HP-UNIX
- \*UNIX\* would **exclude** any value that contains UNIX, e.g. HP-UNIX, HP-UNIX-11, UNIX-11
- UNIX\* would **exclude** any value starting with UNIX, e.g. UNIX-11

- 4 Click in the **Value** cell. If the selected attribute is a list, select the value from the list of values displayed; otherwise, type the value into the cell.




**NOTE** If using a **Like** or **Not Like** constraint, use asterisks as wild cards.

- 5 **apply on link creation only:** Select this option to limit the constraint to when a link is being created.

- 6 Click **OK**.

**To delete a constraint:**

- 1 Highlight the row and click the **Delete** button  in the **Attribute Constraints** area.
- 2 Click **OK**.

**To change an existing constraint rule:**

- 1 Click the cell to be changed and modify the value.
- 2 Click **OK**.

**Suspect Link Rules**

Suspect link rules allow you to mark each side of a specific relationship as suspect when changes occur. If the **mark secondary as suspect on change** check box is selected under **Primary Links**, all secondary links of the relationship type are marked as suspect if the primary object changed. If the **mark primary as suspect on change** check box is selected under **Secondary Links**, all primary links of the relationship type are marked as suspect if the secondary object changed.

When you select either of these check boxes, the **transfer to child** check box is automatically selected.

Note the following:

- Any attribute change causes an object to be marked as suspect.
- There is no relationship between the transfer rules and the suspect link rules; however, they are processed at the same time.
- The object itself is marked as suspect as well as the link. If the object is replaced and it does not have the links transferred, it is no longer linked to the suspect object; however the suspect flag on the object itself still needs to be cleared.

**Populate Attributes Rule**

In some situations it is desirable to populate the attributes of a new object with the values of the attributes of another object. For example, suppose you have a `TestCaseTemplate` class, and you want to use it as a template for all test cases.

**To populate the attributes of a new object with the attributes of an existing object:**

- 1 Create a new class (for example, `TestCase`) and create a relationship from the `TestCaseTemplates` class to the new class.
- 2 Edit the relationship in the **Definition of relationship** dialog box in Class Definition. (In this example, you would select the **populate attributes on create and link** check box for the secondary link.)
  - If the **populate attributes on create and link** check box is selected for the secondary links, the attributes for the object that is secondary in the relationship are populated with attributes based on values in the primary object that already exists.
  - If the **populate attributes on create and link** check box is selected for the primary links, the attributes for the object that is primary in the relationship are populated with attributes based in the values in the secondary object that already exists.

- If the **populate attributes on create and link** check box is selected for both the primary and secondary links, the attributes are populated depending on whether you are linking to the primary object or the secondary object.



#### NOTES

- Only attributes with the same internal name and the same type are populated.
- The default behavior is for the **populate attributes on create and link** check box to be cleared.
- This behavior might not be desirable for all relationships in the schema.

## Specifying Security

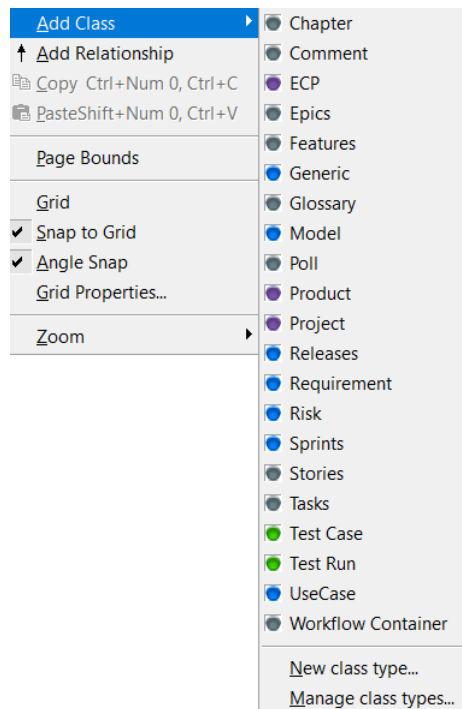
For information about specifying security, see ["Security" on page 320](#).

## Class Types

This section describes how to work with class types.

In **Class Definition**, right-click a blank place in the grid, from the bottom of the menu:

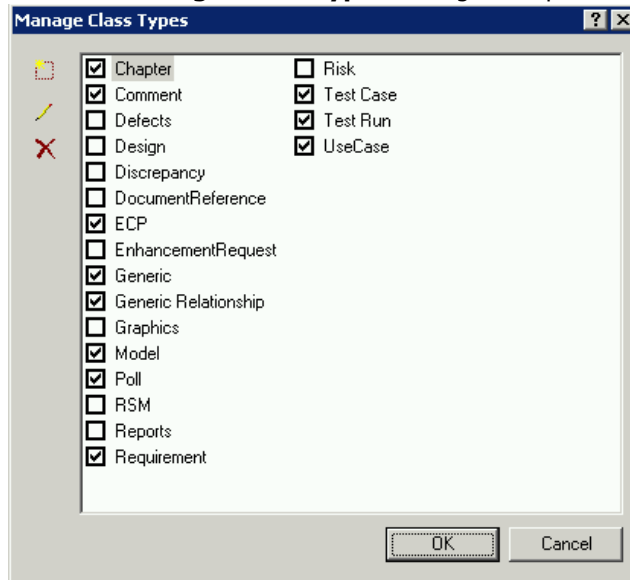
- select **New Class Type** to define a new class type, rather than use one listed
- select **Manage Class Types** to control the class types available for selection



## Manage Class Types

To manage the class types available for selection when defining a new class:

- 1 In **Class Definition**, right-click a blank place in the grid.
- 2 Select **Add Class | Manage class types**.
- 3 The **Manage Class Types** dialog box opens.



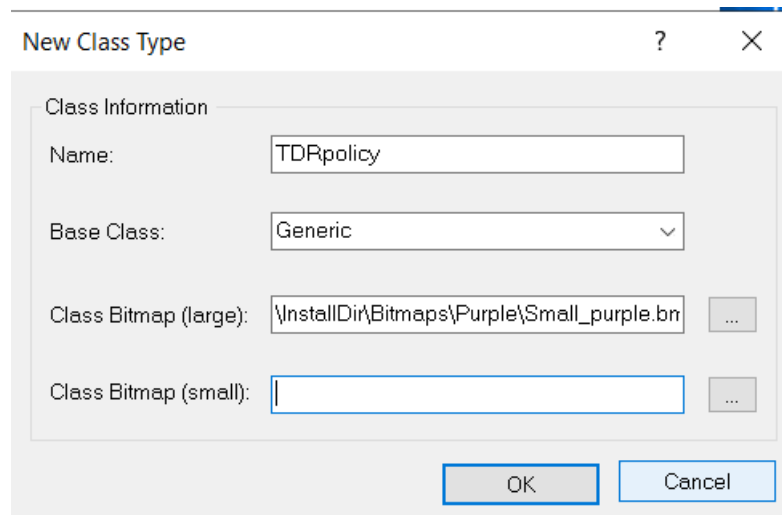
**Figure 9-21. Manage Class Types**

- 4 A selected check box indicates that the class type is valid and will appear on the **Add Class** menu when adding a new class to the schema.
- 5 Click **OK**.

## Adding a New Class Type

To define a new class type definition:

- 1 Select New **Manage Class Types** dialog box. The **New Class Type** dialog box opens.




- Specify properties as described in the following table.

Property	Description
Name	The name of the class type.
Base Class	The class type from which the new class is derived. To create a new class type that has no attributes defined yet, you should derive the class from the Generic class, which contains only the attributes that all class types must have.
Class Bitmap (large)	The large class bitmap field points to the file that is used by Class Definition as the default symbol on the schema diagram.
Class Bitmap (small)	The small class bitmap field points to the file that is used by the Dimensions RM tools to identify the class type.

## Deleting a Class Type

To delete a class type from the instance schema:

- Select the type on the **Manage Class Types** dialog box.
- Click the **Delete** button .



**NOTE** This only removes the type definition. It does not affect any class instances for this type.

## Editing a Class Type Definition

To edit an existing class type definition:

- Select the class type on the **Manage Class Types** dialog box.
- Click the **Edit** button .



**NOTE** This only affects the class type definition. It does not affect any existing class instances of this type.

The **Definition of class** dialog box opens.

## Specifying Attributes

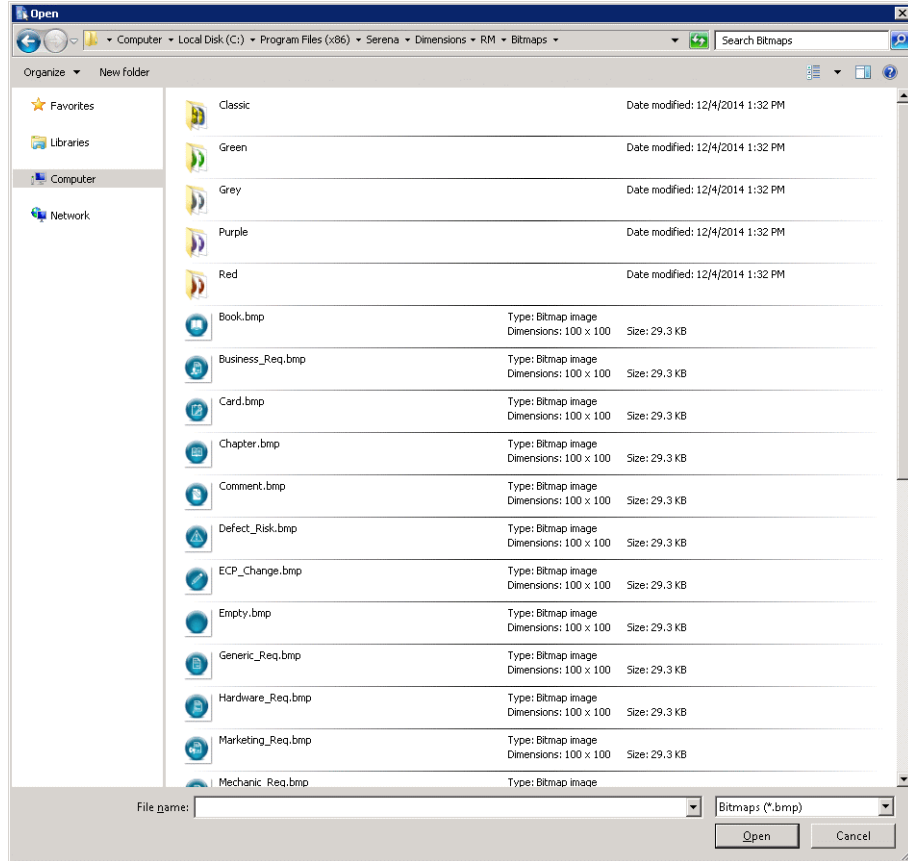
For information about specifying attributes, see ["Attributes" on page 275](#).

## Changing the Class Definition Bitmap

Class Definition allows the user to define the image that is used on the schema diagram as well as associate a small bitmap that will be used by the other tools to identify the class type.

**To change the image:**

- 1 Right-click the image and select **Change Image**.



**Figure 9-22. Class Type Definition Visual**

- 2 Locate the Windows bitmap file containing the image. A preview of the bitmap appears on the main property page.



**NOTE** There are no constraints on the size of the bitmap, but for performance, the size should be reasonable and the image should only be up to 8-bit color.

## Changing the Class Icon

To change the icon used to represent a class type, click **Open** to the right of the **File name** list and locate the Windows bitmap file. A preview of the bitmap is displayed on the main property page. The bitmap should be 16x16 pixels and 8-bit color.

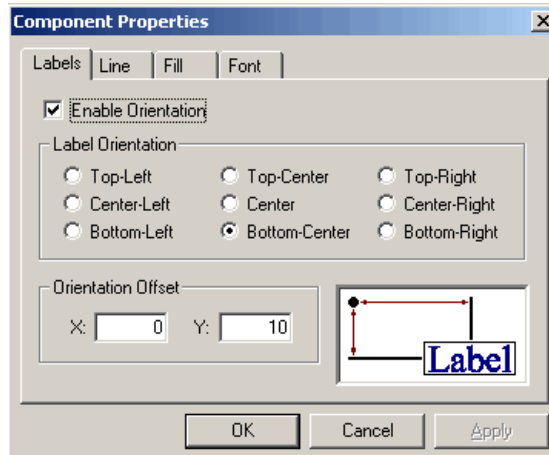


**NOTE** Only bitmaps of up to 8-bit color can be used.

## Changing the Label Properties for Class Types

To change the default properties for the label associated with a class type:

- 1 In **Class Definition**, right-click the object and select **Properties**. The **Component Properties** dialog box opens.
- 2 Click the **Labels** tab.



**Figure 9-23. Component Properties**

- 3 Customize the format of the label for the class type.

## Security



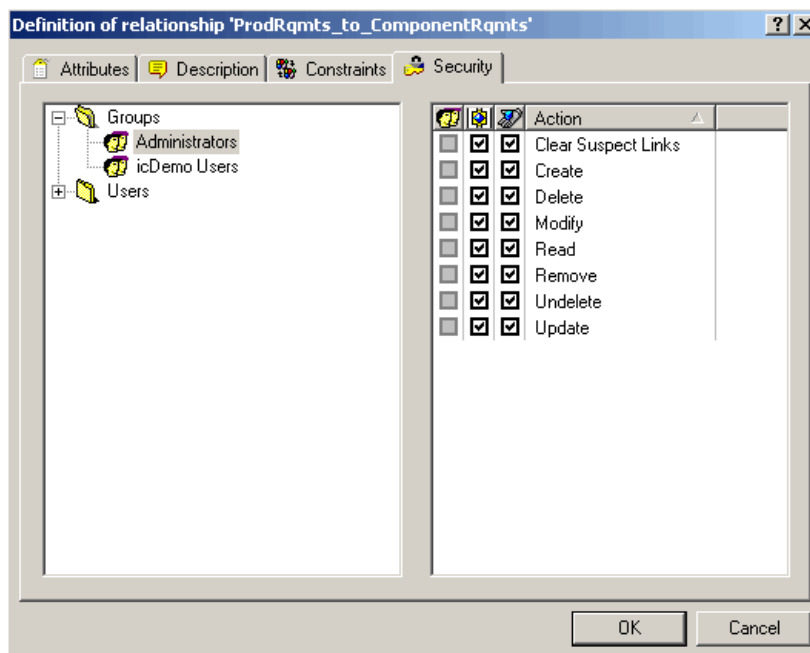
**IMPORTANT!** Access rights and category permissions are now controlled by the Instance Administrator in RM Browser. It is necessary for the administrator, when creating a new schema, to grant access to the one or more instance administrators, but all further permissions should be granted from the Administration menu: **Manage User/Groups**.

### Granting Group Access

Historically, it has been possible to modify user and group access from each class from Class Definition. This functionality is still supported, but is not for the faint of heart. Best practice is to manage group, user and category access from the browser.

- 1 To change the access of a group to the selected resource:
- 1 In **Class Definition**, right-click the resource and select **Define**.




- 2 Click the **Security** tab.



**Figure 9-24. Definition of Relationship—Security Tab**

- 3 Click + next to **Groups**.
- 4 Select the group.
- 5 Click the required transaction to toggle the access rights. For group access rights the group is allowed  or denied  access.
- 6 Click **OK**.
- 7 Save the instance schema.

#### Access Rights:

- |   |                 |   |
|---|-----------------|---|
|  | <b>Group</b>    | The <b>Group</b> setting defines if all users of a group gain access. Note that the <b>Group</b> setting cannot deny a right gained on instance level.        |
|  | <b>Instance</b> | The <b>Instance</b> column shows the right gained on instance level. Note that you cannot change the right here.  |
|  | <b>Actual</b>   | The <b>Actual</b> setting defines the actual right of the group. Note that the <b>Actual</b> box is always selected if the right is gained on instance level. |

## Valid Actions

The tables in the following sections list the valid Actions for classes, relationships, and source documents.

### Valid Actions for Classes

The following table lists the valid transactions for classes and describes what the transactions allow a user or group to do.

Transaction	Description
CM Lock	Define the class object as CMLocked (configuration management locked).
Create	Create objects for the class.
CreateCR	Create new change requests for objects in the class. <b>NOTE:</b> To create change requests, a user or group must have explicit access to the "CreateCR" and "Read" actions at the class level, and to the "Read" action at the relationship level.
Delete	Mark the class objects as deleted. When using documents, the <b>Delete</b> right is required on the <b>Chapter</b> class if users are to delete chapters. Note that before Dimensions RM 12.6.1, the <b>Remove</b> right was used instead.
ExecuteCR	Accept or reject change requests.
Execute Transition	The user can execute any transition of any class.
Execute Transition if Owner	The user can execute any transition if he or she owns the requirement.
Execute Transition if Submitter	The user can execute any transition if he or she submitted the requirement.
Expand	Expand class objects.
Focus	Focus class objects.
Link	Create generic links to the class objects.
Provide To	The user can branch requirements.
Read	Read the class objects.
Remove	Remove the class objects.
Replace	Replace the class objects.
Synchronize To	The user can merge branched requirements.
Undelete	Undelete the class objects.
Unlock	Unlock the class objects that are locked.
Update	Update the class objects with a status of Current.
UpdateCR	The user can update an object with a status of "Proposed."
Update NonCurrent	Update the class objects with a status other than Current.

### Valid Transactions for Relationships

The following table lists the valid transactions for relationships and describes what the transactions allow a user or group to do.

Transaction	Description
Clear Suspect Links	The user can clear suspect links of one requirement at a time.
Create	The user can create new links for relationships.
Delete	The user can delete links for relationships.
Mass Clear Suspect Links	The user can delete suspect links of one or several requirements at a time.
Modify	The user can change relationship attribute values.
Raise Suspect Links	The user can make a linked requirement suspect.
Read	The user can look at relationship links.
Remove	The user can remove relationship links.
Undelete	The user can undelete relationship links.
Update	The user can update relationship links with a status of "Current".

### Valid Transactions for Source Documents

The following table lists the valid transactions for source documents and describes what the transactions allow a user or group to do.

Transaction	Description
Capture	Capture class objects from documents.
Create	Register new documents.
Read	View registered documents.
Remove	Unregister documents.
Unlock	Unlock documents.

## Saving the Instance Schema



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

Best practice is to use the Schema Definition in RM Browser to modify the schema from client systems.

To save the instance schema, select **File | Save** or click the **Save**  button.

If there are one or more users currently working with other tools in the instance you have changed, the **Tool Locks** dialog is displayed, identifying the names and computers of the current users, as well as the tools they are using.

You can cancel the save operation until other users have finished working, or you can click **Remove All** to remove the tool locks - but this should only be done if you are sure that the lock has been left by someone no longer working in the schema.

## Reloading the Instance Schema

If changes have been made to the instance schema since the last save operation, you can discard them by selecting **File | Reload**. This discards all changes and reloads the instance schema. If you are an instance administrator, **Reload** locks the instance schema so that changes can be made.

## Releasing the Instance Schema Lock

If the instance schema is loaded in read/write mode and you do not want to make changes, the schema lock can be released by selecting **Release Lock** from the **File** menu. This allows another user to make changes to the instance schema while you are still able to view the read-only version. If any changes have been made, you will be warned that the changes will be lost, and will be allowed to save the changes or cancel the operation.

## Deploying the Instance Schema

It is typical for analysts within the organization to define "the perfect basis schema" to be shared with all new instances. Individual applications teams may choose to add or hide attributes, but there will remain a single shared schema that defines requirements using the corporate lexicon.

The System Administrator is responsible for deploying the Instance Schema. it is possible to:

- Deploy a schema to an instance defined in the same database or on the same network. After deployment, it becomes the responsibility of the Instance Administrator to perform Administration Tasks, e.g. adding groups, users, and defining permissions.
- Deploy a schema to an instance on a separate network. This process uses a combination of backup and restore in conjunction with deploy, and is typically used to deploy a schema from Test to Production after testing changes.

To deploy the schema from one instance to another on the same network, see: ["Deploying the Schema Locally" on page 325](#).

To deploy the schema across the network, see ["Deploying the Schema Across the Network" on page 325](#).



### CAUTION!

**Create a backup** of the target machine's instance(s) before deploying the schema. This backup should include the data.

Classes which are not present in the source instance are deleted in the target instance when the schema is deployed. This also removes the data of these classes.

**If security permissions are copied**, the security permissions for groups on the target are overwritten.

## Deploying the Schema Locally

- 1 In **RM Manage**, select **File | Deploy Schema**. This opens the **Select Destination Instance(s)** dialog.
- 2 Select one or several instances to deploy.
- 3 Click **OK**. This opens the **Schema Deployment** dialog. This dialog shows the changes that will take place when deploying the schema. If you selected several instances to deploy to, click ► next to an instance name to view the changes for that instance.
- 4 By default, security permissions are copied. To prevent that security permissions are copied, do the following:
  - a Click **Settings**. This opens the **Deploy Settings** dialog.
  - b Clear the **Include Security Permissions** option.
  - c Click **OK**.
- 5 Review the changes.
- 6 Click **Deploy** to start schema deployment. After deployment is complete, the **Schema Deployment** dialog shows the success message.
- 7 Click **Close**.

## Deploying the Schema Across the Network

To enable the Instance Schema for deployment in another database. For example, when moving tested schema updates from test to production.

- 1 Backup the Instance selected for deployment (see ["Dimensions RM Backup" on page 182](#)) ["Dimensions RM Backup" on page 182](#), using either schema or account backup. Copy the backup to the targeted server.
- 2 Create an new instance, e.g. Test, in the target server.

- 3 Restore the backup into the new instance, and use Deploy to copy changes into the selected target.



**NOTE** If instance changes will be deployed again using this approach, it might be simpler to leave the new instance on the production server. If you choose to do this, we recommend that you place the instance offline (right click on the instance and choose 'Place Instance Account Offline') so that it is available for the next deployment without the possibility of any user accessing it.

- 4 In **RM Manage**, select **File | Deploy Schema**. This opens the **Select Destination Instance(s)** dialog.
- 5 Select one or several instances to deploy.
- 6 Click **OK**. This opens the **Schema Deployment** dialog. This dialog shows the changes that will take place when deploying the schema.  
If you selected several instances to deploy to, click ► next to an instance name to view the changes for that instance.
- 7 By default, security permissions are copied. To prevent that security permissions are copied, do the following:
  - a Click **Settings**. This opens the **Deploy Settings** dialog.
  - b Clear the **Include Security Permissions** option.
  - c Click **OK**.
- 8 Review the changes.
- 9 Click **Deploy** to start schema deployment. After deployment is complete, the **Schema Deployment** dialog shows the success message.
- 10 Click **Close**.

## Printing the Instance Schema Diagram

**To print the instance schema:**

- 1 In **Class Definition**, select **File | Print** or click the **Print** button .
- 2 Select print options.
- 3 Click **OK**.

## Printing the Instance Schema Definitions

You can print definitions for each of the classes and relationships to a printer or to an RTF file.

**To print instance schema definitions:**

- 1 In **Class Definition**, select **Print Definitions** from the **File** menu.

- 2 Select the definitions you would like to print.
- 3 Click **Next**.
- 4 Select how you would like to print the definitions. You have four types of options: class, relationship, form, and source document. These options allow you to select which class or relationship definitions will be printed, and which data will be printed.
- 5 Click **Next**.
- 6 Click **Print**.
- 7 Click **Finish** to exit.



**NOTE** On the preview page you can choose to save the output to an RTF file, which can subsequently be formatted using an RTF-capable editor such as WordPad.

## Implementing Suspect Links

To implement the suspect links feature, use Class Definition to define constraints and security on relationships.



**NOTE** For detailed information about the suspect links feature, see the *Dimensions RM Browser User's Guide*.

### To implement the suspect links feature:

- 1 Specify suspect link constraints on the relationships that you want to participate in the suspect links feature. For more information, see "[Specifying Constraints](#)" on page 311.
- 2 Specify the **Clear Suspect Links** action for each user and group that should have permission to clear suspect links. For more information, see "[Security](#)" on page 320.

## Defining the Date Format

When you define a date attribute in the **Date Attribution Definition** dialog box, the display format for the date can also be defined. This format will be used for both displaying the date attribute, and validating the date attribute when entering a new value.

**To define the date format:**

- Select or type a format in the **Display Format** box.

**Figure 9-25. Date Attribute Definition Dialog**

## Date Format Elements

When entering a new date any of the format elements shown below can be used, but format items cannot appear twice and also format items that represent similar information cannot be combined. For example, you cannot use "SYYYY" and "BC" in the same format string.

Element	Meaning
D	Day of week (1-7)
J	Julian day; the number of days since January 1, 4712 BC. Numbers specified with "J" must be integers.
Q	Quarter of year (1,2,3,4; 1=January–March)
W	Week of month (1-5) where week 1 starts on the first day of the month and ends on the seventh
AD A.D.	A.D. indicator with or without periods
AM A.M.	Meridian indicator with or without periods
BC B.C.	B.C. indicator with or without periods
PM P.M.	Meridian indicator with or without periods
CC SCC	Century; "S" prefixes BC dates with "-"

Element	Meaning
DD	Day of month (1-31)
DY	Abbreviated name of day
IW	Week of year (1-52 or 1-53) based on the ISO standard
MI	Minute (0-59)
MM	Month (01-12; Jan=01)
RM	Roman numeral of month (I-XII; Jan=I)
WW	Week of year (1-53) where week 1 starts on the first day of the year and continues to the seventh day of the year
SS	Second (0-59)
DAY	Name of day, padded with blanks to length of 9 characters
DDD	Day of year (1-366)
MON	Abbreviated name of month
IYY IY I	Last 3, 2 or 1 digit(s) of the ISO year
YYY YY Y	Last 3, 2, or 1 digit(s) of year
Y YYY	Year with comma in this position
HH HH12	Hour of the day (1-12)
HH24	Hour of the day (0-23)
MONTH	Name of month, padded with blanks to length of 9 characters
IYYY	4-digit year based on the ISO standard
RRRR	4-digit year; allows entry of 2 digit year and calculates century based on the 2 digit year value entered. See " <a href="#">RRRR Date Format Elements</a> " on page 330. <b>NOTE:</b> This is the preferred format for 4-digit years.
SSSSS	Seconds past midnight (0-86399)
YEAR SYEAR	Year spelled out; "S" prefixes BC dates with "-"
YYYY SYYYYY	4-digit year; "S" prefixes BC dates with "-"

## Date Format Element Suffixes

The following table lists suffixes that can be added to date format elements:

Suffix	Meaning	Example Element	Example Value
TH	Ordinal Number	DDTH	4TH
SP	Spelled Number	DDSP	FOUR
SPTH or THSP	Spelled, Ordinal Number	DDSPTH	FOURTH

When you add one of these suffixes to a date format element, the return value element is always in English.



**NOTE** Date suffixes are only valid on output and should not be used when entering a date (for example, a date attribute with the format defined as "DDTH Mon, YYYY" will be displayed as "12th Jan, 1999" but should be entered as "12 Jan, 1999").

## Capitalization of Date Format Elements

Capitalization in a spelled-out word, abbreviation, or Roman numeral follows capitalization in the corresponding format element. For example:

- "DAY" produces "MONDAY"
- "Day" produces "Monday"
- "day" produces "monday"

## RRRR Date Format Elements

The RRRR date format element is similar to the YYYY date format element, but it provides additional flexibility for storing date values in other centuries when you enter a two-digit year. For example, it allows you to store twenty-first century dates in the twentieth century when you specify only the last two digits of the year.

The following table describes the behavior of the RRRR date format element.

Last Two Digits of Current Year	Digits Entered in Oracle	Century in which Date is Created
00-49	00-49	Current
	50-99	Prior
50-99	00-49	Next
	50-99	Current

The following table provides examples of this behavior.

Current Year	Digits Entered in Oracle	Date Created
2004	09	2009
	99	1999
2094	09	2109
	99	2099

## Punctuation and Character Literals in Date Format Models

You can also include these characters in a date format model:

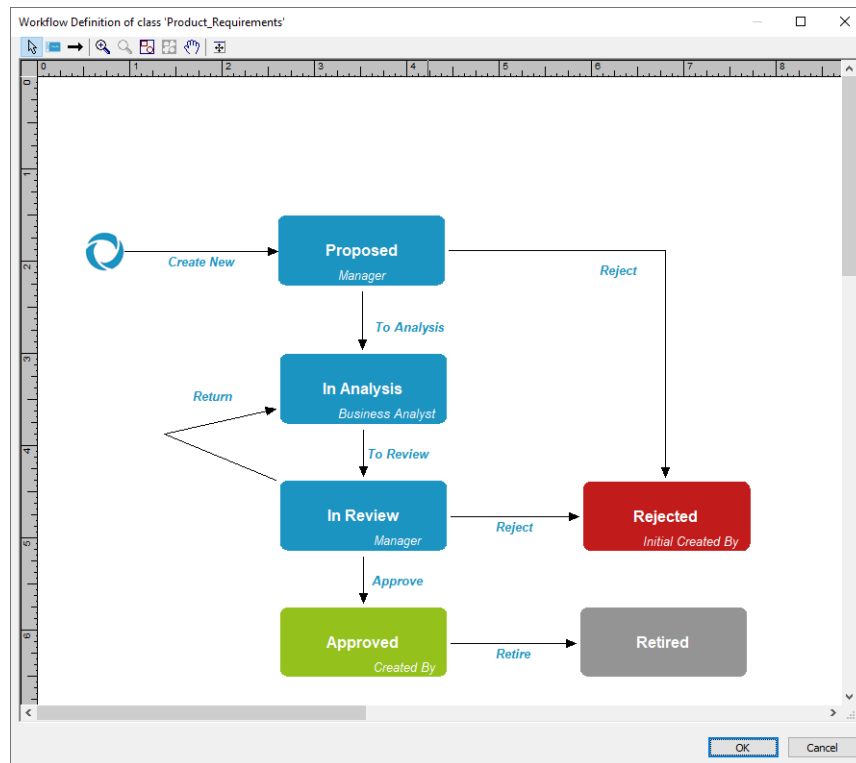
- Punctuation marks such as hyphens, slashes, commas, periods, and colons
- Character literals

These characters appear in the displayed value in the same location as they appear in the format model, and must be entered in the same location for a new date value to be valid.

## Workflows

A workflow ensures the proper flow of requirements using a defined process that consists of attributes, states and transitions. Requirements must follow this workflow from the

time they are submitted. You design workflows in the Workflow Definition Designer of the Class Definition tool.



**Figure 9-26. Workflow for class `Product_Requirements`**

## Workflow Elements

A workflow consists of two elements: states and transitions.

**State:** A state is a position in a workflow where a requirement resides. While a requirement resides in a given state, it has an owner who is responsible for performing a specific task with the requirement.

**Transition:** A transition activates the movement of a requirement from one state to another in the workflow.

## Creating or Editing a Workflow

You can create workflow only for a class. It is not possible to create one workflow which handles several classes.

**To create a workflow, follow these steps:**


- 1 Start the **Class Definition** tool.
- 2 Log in with an administrator account.
- 3 Right-click the desired class and select **Define** from the shortcut menu.
- 4 Ensure that the **Enable Workflow** box is selected.

- 5 Click the **Workflow Definition** button. This opens the Workflow Definition Designer.
- 6 Design your workflow by adding, modifying or deleting states and transitions.
- 7 Click **OK** to close the Workflow Definition Designer.
- 8 Click **OK** to close the *Definition of class 'Class Name'* dialog.
- 9 Save the class definition.

## **Workflow States**

### **Adding a Workflow State**

To add a state, follow these steps:

- 1 Click the  button in the toolbar. Alternatively, you can right-click the work area and select **Add State** from the shortcut menu.
- 2 Click the position of the work area where you want the state to be located.
- 3 Enter a state name and press **Enter**.



**NOTE** State names must be unique.



**TIP** You can move a state or transition by selecting it and pressing the arrow keys on your keyboard.

### Changing a Workflow State Name

To change a state name, double-click the name and enter the new name. Then, press **Enter**.



**NOTE** State names must be unique.

### Changing a Workflow State Definition

To change a state definition you can either double click the state or right-click the state and select **Define...** from the shortcut menu. This opens the *Definition of state 'State Name'* dialog which allows you to change these definitions:

- [Common Settings](#)
- [Description Text](#)
- [Form Settings](#)
- [Security Settings](#)

#### *Common Settings*

The Common settings dialog is opened when you open the *Definition of state 'State Name'* dialog. To change Common settings after you changed other settings, select the **Common** tab. The Common settings dialog allows you to change the following settings:

- **Owner:** Changing the owner can prevent that other users cannot execute any transaction on this state. This depends on the configuration of the attribute (i.e. single user, group or team), user/group access rights, and security settings for the transition.
- **Progress:** This setting is only available with container workflows. The specified progress value is shown as a progress bar in the Document View.
- **Order:** Allows you to specify the order in which transition buttons are shown on transition forms.

#### *Description Text*

To change the description text, select the **Description** tab. The description is shown as a tool tip for each state in the requirement's state history.

#### *Form Settings*

To change the form settings, select the **Form** tab. The Forms settings dialog provides two lists:

**Sections:** Defines which sections are shown when the user opens the requirement.

**User Defined Attributes:** Defines how to process user defined attributes.

Setting	Description
Display	<p>Display the attribute if its parent section is also displayed.</p> <p><b>NOTE</b> If you choose to hide (not display) attributes on selected workflow forms, please test the display.</p> <ol style="list-style-type: none"> <li>1 Check to ensure that the modified display will not confuse users.</li> <li>2 If using modified forms, consider how the form will appear after the display of some attributes is suppressed. You might consider placing suppressed attributes into a single section. This will allow suppression of the section without affecting the display of other attributes on the form.</li> </ol>
Editable	The attribute can be changed
Mandatory	The attribute must have a value.

### Security Settings

To change the security settings, select the **Security** tab. The security settings define which user or group can read, replace or update a requirement of the selected state.

Transaction	Definition
Read	The user can see the data of the requirement.
Replace	The user can replace attribute values of the requirement.
Replace if Owner	The user can replace attribute values of the requirement if he or she owns it.
Update	The user can update attribute values of the requirement.
Update if Owner	The user can update attribute values of the requirement if he or she owns it.

For further information about security settings, see chapter ["Security" on page 320](#).

### Deleting a Workflow State

To delete a state, follow these steps:

- 1 Select the state you want to delete.
- 2 Press the **Delete** key or right-click the state and select **Delete** from the shortcut menu.
- 3 Confirm the following dialog.





**NOTE** A state can only be deleted if no requirement is within that state.

## Ordering Workflow Transitions

If you have several transitions with a state, you may want them to be in a certain order (e.g. mostly used transition to the left, least used to the right).

To change the transition order, do the following:


- 1 Double-click the state for which you want to change the transition order. This opens the **Definition of state** dialog.
- 2 Ensure that the **Common** tab is selected.
- 3 Select a transition and click  or  to change the position of the transition. Repeat this for other transitions until you have the desired order.
- 4 Click **OK**.

## Workflow Transitions

### Adding a Workflow Transition

In order to add a transition you need at least 2 states in your workflow diagram.

**To add a transition, follow these steps:**

- 1 Click the  button in the toolbar. Alternatively, you can right-click the work area and select **Add Transition** from the shortcut menu.
- 2 Click the state you want the transition to start from.
- 3 Click the state you want the transition to end.



**TIP** You can create a "angled" transition arrow (e.g. a 90° angle) by clicking at several points in the work area before clicking the end state.

- 4 Enter a transition name and press **Enter**.



**TIP** You can move a state or transition by selecting it and pressing the arrow keys on your keyboard.

### Changing a Workflow Transition Name

To change a transition name, double-click the name and enter the new name. Then, press **Enter**.

### Changing a Workflow Transition Definition

To change the transition definition you can either double click the transition arrow or right-click the transition arrow and select Define... from the shortcut menu. This opens the *Definition of transition 'Transition Name'* dialog which allows you to change these definitions:

- [Description Text](#)
- [Form Settings](#)

- [User Field Settings](#)
- [Attribute Constraint Settings](#)
- [Relationship Constraint Settings](#)
- [Security Settings](#)

#### *Description Text*

To change the description text, select the **Description** tab. The text you enter is used as a tool tip which pops up when the user hovers the button for that transition.

#### *Form Settings*

To change the form settings, select the **Form** tab. The Form settings allow you to define if a transition is a regular or a quick transition. Quick transitions do not show any form, so users cannot modify any attributes of a requirement. To turn a regular transition into a quick transition, select the **Quick Transition** box. If you clear the **Quick Transition** box, the Forms settings dialog provides two lists:

**Sections:** Defines which sections are shown when the user opens the requirement.

**User Defined Attributes:** Defines how to process user defined attributes.

Setting	Description
Display	Display the attribute if its parent section is also displayed.  <b>NOTE</b> If you hide attribute controls, the attribute controls following the hidden attribute controls may be re-arranged. This may be confusing to some users.
Editable	The attribute can be changed
Mandatory	The attribute must have a value.
Clear Value	Clears the value of the attribute.

When executing a transition, you can also require an electronic signature. This means that the user has to confirm his identity by entering user name and password. To enable electronic signature for a transition, select the **Electronic Signature** box.

When using electronic signatures with a transition, the following data will be stored:

- User name and user ID
- Timestamp of transition was executed
- Executed transition

#### *User Field Settings*

When executing a transition, user fields can be modified. All options contain a list of the current user fields. You can use this function, for example, to see update an attribute (e.g. Reviewer) during a review workflow. This would allow you to see which user reviewed a requirement.

**The following options are available:**

- **Remove current user from user field(s):**
  - **Single value list:** If any of the selected user attributes holds the user executing the transition, the user attribute will be cleared.
  - **Multiple values list:** If the user executing the transition is selected in the selected user fields, the user will be deselected.
- **Add current user to user field(s):**
  - **Single value list:** The selected user attributes will be show the user executing the transition.
  - **Multiple values list:** Selects the current user in the selected user attributes.
- **Remove selection from user field(s):**
  - **Single value list:** The selected user attributes will be cleared.
  - **Multiple values list:** All users will be deselected on the selected user attributes.



\*UNIX, \*UNIX\*, or UNIX\* would match with these attributes: HP-UNIX, HP-UNIX-11, or UNIX-11.

- **Null** The attribute does not contain a value.
  - **Not Null** The attribute contains a value.
- 3 Click in the **Value** cell. If the selected attribute is a list, select the value from the list of values displayed; otherwise, type the value into the cell.



**NOTE** If using a **Like** constraint, use asterisks as wild cards.


- 4 If desired, click into the **Automatic** cell and select a different value from the drop-down menu. The following selections are available:
- **No:** The transition is executed by clicking the transition button.
  - **Yes:** The transition is executed automatically if the requirement is in state "Current". The user interface shows no button for the transition.



**CAUTION!** It is not recommended to use automatic execution on several transitions originating from the same Workflow state. If the constraints of several transitions are true, it cannot be predicted, which of these transitions Dimensions RM will execute.

- 5 Click **OK**.

**To delete an attribute constraint:**

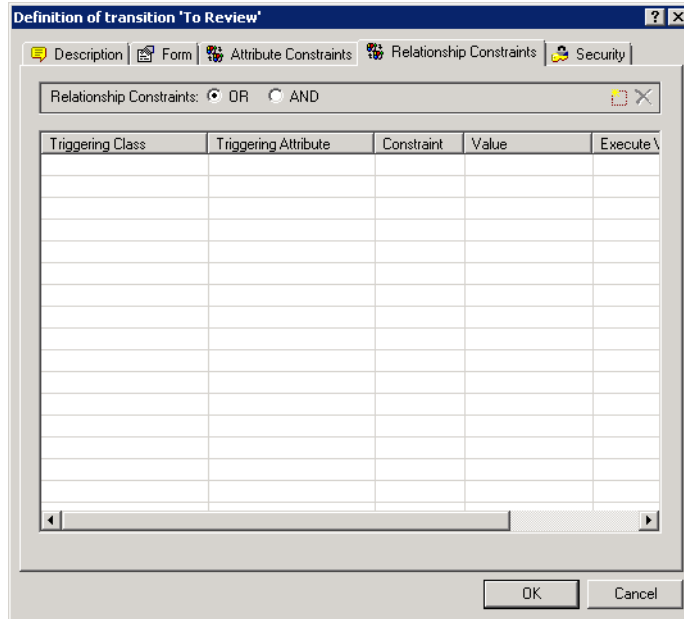
- 1 Highlight the row and click the **Delete** button  in the **Attribute Constraints** area.
- 2 Click **OK**.

**To change an existing attribute constraint rule:**

- 1 Click the cell to be changed and modify the value.
- 2 Click **OK**.

*Relationship Constraint Settings*

To change the relationship constraint settings, select the **Relationship Constraints** tab. By creating or modifying constraints you define under which conditions the transition can be executed.



**Figure 9-28. Relationship Constraint Settings dialog**



#### NOTES

- Relationship Constraints are checked when clicking the associated button.
- Relationship constraints that have been defined on a transition are different from relationship constraints that have been defined on relationship level.




**TIP** You can use the relationship constraint also to automatically execute a transition for all requirements of a document. You might, for example, use this function in an approval process in which you want to approve all requirements of a document.

To configure the described automatic transitioning of requirements, edit the Workflow Relationship Constraints for each class and reference the workflow of the container in the **Triggering Class** column.

#### To add relationship constraints:

- 1 Click **OR** or **AND** in the **Relationship Constraints** area to specify the type of logical relationship you are about to specify.
- 2 Specify the constraints as described in the following sections.
- 3 Click **OK**.

#### To add a new relationship constraint:

- 1 Click the **New Constraint** button  in the **Relationship Constraints** area to add a new row to the table.

- 2 Click into the **Triggering Class** cell and select the class from the drop-down menu for which you want to define the constraint.
- 3 Click into the **Triggering Attribute** cell and select the attribute from the drop-down menu for which you want to define the constraint.
- 4 Click in the **Constraint** cell and select the desired constraint type from the drop-down menu. The following constraint types are available:
  - = The attribute *exactly* equals the value.
  - != The attribute does NOT equal the value.
  - **Like** The attribute includes the value as part of a larger string. When using Like, you would include one or more asterisks (\*) as wild cards to indicate where the value fits into the larger attribute string. For example, taken in order, these values: \*UNIX, \*UNIX\*, or UNIX\* would match with these attributes: HP-UNIX, HP-UNIX-11, or UNIX-11.
- 5 Click in the **Value** cell. If the selected attribute is a list, select the value from the list of values displayed; otherwise, type the value into the cell.



**NOTE** If using a **Like** constraint, use asterisks as wild cards.


- 6 If desired, click into the **Execute When** cell and select a different value from the drop-down menu. The following selections are available:
  - **At least one:** Executes the transition if one linked requirement fulfills the constraint.
  - **All:** Executes the transition if all linked requirements fulfill the constraint.
  - **All or Not Linked:** Executes the transition if all linked requirements fulfill the constraint or no requirements of the class (specified in the **Triggering Class** cell) are linked.
- 7 If desired, click into the **Automatic** cell and select a different value from the drop-down menu. The following selections are available:
  - **No:** The transition is executed by clicking the transition button.
  - **Yes:** The transition is executed automatically if the requirement is in state "Current". The user interface shows no button for the transition.



**CAUTION!** It is not recommended to use automatic execution on several transitions originating from the same Workflow state. If the constraints of several transitions are true, it cannot be predicted, which of these transitions Dimensions RM will execute.

- 8 Click **OK**.

#### To delete an relationship constraint:

- 1 Highlight the row and click the **Delete** button  in the **Relationship Constraints** area.
- 2 Click **OK**.


**To change an existing relationship constraint rule:**

- 1 Click the cell to be changed and modify the value.
- 2 Click **OK**.

**Use Case: Automatic Transitioning Requirements with a Container Workflow**

This use case describes how to transition requirements that are in a container (document, snapshot, collection, or baseline) to a new Workflow state. For the steps below, the RMDEMO instance is used. When transitioning the container, the requirements will also be transitioned.

**To configure automatic transitioning of requirements:**

- 1 Start the Class Definition tool as described in chapter ["Starting Class Definition" on page 270](#).
- 2 Open the class (e.g. *Product\_Requirements*) containing the workflow you want to modify by using one of these methods:
  - Double-click the class
  - Right-click the class and select **Define...** from the shortcut menu
- 3 Open the workflow by clicking the **Workflow Definition** button.
- 4 Open the transition you want to execute (e.g. *Approve*) by using one of these methods:
  - Double-click the transition
  - Right-click the transition and select **Define...** from the shortcut menu
- 5 Select the **Relationship Constraints** tab.
- 6 Click  in the **Relationship Constraints** area to add a new row to the table.
- 7 Click into the **Triggering Class** cell and select the container workflow class (e.g. *Approval*) from the drop-down menu for which you want to define the constraint.
- 8 Click into the **Triggering Attribute** cell and select the **Workflow State** attribute from the drop-down menu.
- 9 Ensure that the **Constraint** cell shows =.
- 10 Click into the **Value** cell. Select the workflow state to which you transition the requirement (e.g. *Approved*).
- 11 Ensure that the **Execute When** cell shows **At least one**.
- 12 Scroll to the right, click into the **Auto** cell and select **Yes**.



**CAUTION!** It is not recommended to use automatic execution on several transitions originating from the same Workflow state. If the constraints of several transitions are true, it cannot be predicted, which of these transitions Dimensions RM will execute.

- 13 Click **OK** to close the **Definition of transition** dialog.
- 14 Click **OK** to close the **Workflow Definition** dialog.

- 15 Click OK to close the **Definition of class** dialog.
- 16 Modify any other workflows if required.
- 17 Save your schema definition.

### Security Settings

To change the security settings, select the **Security** tab. The security settings define which user or group can execute a transition of the selected state.

Transaction	Definition
Execute Transition	The user can execute this transition.
Execute Transition if Owner	The user can execute this transition if he or she owns the requirement.
Execute Transition if Submitter	The user can execute this transition if he or she submitted the requirement.

For further information about security settings, see chapter ["Security" on page 320](#).

### Deleting a Workflow Transition

To delete a transition, follow these steps:

- 1 Select the transition you want to delete.
- 2 Press the **Delete** key or right-click the transition and select **Delete** from the shortcut menu.
- 3 Confirm the following dialog.

## Copying a Workflow to another Class

A workflow can be copied from one class to another class. The copied workflow will contain all states and transitions of the original workflow.

**To copy a workflow to another class, follow these steps:**

- 1 Start the **Class Definition** tool.
- 2 Log in with an administrator account.
- 3 Right-click the desired class having a workflow and select **Copy Workflow** from the shortcut menu. This opens the **Select Destination Class** dialog.
- 4 Select the class to copy the workflow to.
- 5 Click **OK**.
- 6 Confirm the success message.

- 7 Save your class definition.

**NOTE**

- You cannot copy a workflow if the target class already contains a workflow and there are requirements using that workflow.
- If the source class contains attributes which are not defined in the target class, the workflow constraints and form settings for these attributes are ignored.
- If the target class contains attributes which are not defined in the target class, the workflow will use the defaults for these attributes.
- Security settings are not copied.

## Deleting a Workflow

A workflow can only be deleted if there are no requirements within any state of that workflow. If this is not the case, the workflow can only be disabled.

**To delete a workflow, follow these steps:**

- 1 Start the **Class Definition** tool.
- 2 Log in with an administrator account.
- 3 Right-click the desired class and select **Define** from the shortcut menu.
- 4 Click the **Workflow Definition** button. This opens the Workflow Definition Designer.
- 5 Delete all states and transitions except the **New** state.
- 6 Click **OK**.
- 7 Clear the **Enable Workflow** box.
- 8 Click **OK** to close the Workflow Definition Designer.
- 9 Click **OK** to close the *Definition of class 'Class Name'* dialog.
- 10 Save your class definition.

**To disable a workflow, follow these steps:**

- 1 Start the **Class Definition** tool.
- 2 Log in with an administrator account.
- 3 Right-click the desired class and select **Define** from the shortcut menu.
- 4 Clear the **Enable Workflow** box.
- 5 Click **OK**.
- 6 Save your class definition.

## Using Containers with Workflows

If you want to use containers (documents, collections, and baselines) with Workflows, you must create a class of type **WorkFlow\_Container**. By using containers with workflows you could define an approval process for that container.

### Creating the WorkFlow\_Container Class

To create the **WorkFlow\_Container** class, do the following:

- 1 Start **RM Manage**.
- 2 Expand the database in which your instance resides.
- 3 Fill the fields of the **Logon Information** dialog and click **OK**.
- 4 Right-click your instance and select **Define Instance Schema** in the shortcut menu.
- 5 In the **Class Definition** dialog, right-click on a free space and select **Add Class | WorkFlow Container** from the shortcut menu.
- 6 Click on a free space to place the new class.
- 7 Change the name to your liking, e.g. *WorkFlow\_Container*.
- 8 You can extend the definition of the *WorkFlow\_Container* class by adding custom attributes. For further information on adding attributes, see chapter "[Adding an Attribute](#)" on page 295.
- 9 Add a workflow to the *WorkFlow\_Container* class as described in chapter "[Creating or Editing a Workflow](#)" on page 332.
- 10 Save the class definition.

### Configuring Progress for States

For states within the *WorkFlow\_Container* class, you can define progress which is shown when the document, collection, or baseline is shown.



**NOTE** The progress is not stored for each container individually, but for the state only. Changing the progress at a later time will result in a changed progress displayed for all containers in that state.

To define progress for a state, do the following:

- 1 Start **RM Manage**.
- 2 Expand the database in which your instance resides.
- 3 Fill the fields of the **Logon Information** dialog and click **OK**.
- 4 Right-click your instance and select **Define Instance Schema** in the shortcut menu.
- 5 In the **Class Definition** dialog, double-click the *WorkFlow\_Container* class. This opens the **Definition of class 'WorkFlow\_Container'** dialog.
- 6 Click **Workflow Definition**. This opens the **Workflow Definition of class 'WorkFlow\_Container'** dialog.

- 7 Double-click the state for which you want define the progress. This opens the **Definition of state 'State Name'** dialog.
- 8 Fill the desired percentage into the **Progress** box. Note that you can only use integer numbers here.
- 9 Click **OK** to close the **Definition of state 'State Name'** dialog.
- 10 Repeat steps 7-9 for other states if desired or required.
- 11 Click **OK** to close the **Workflow Definition of class 'WorkFlow\_Container'** dialog.
- 12 Click **OK** to close the **Definition of class 'WorkFlow\_Container'** dialog.
- 13 Save the class definition.

## Creating Product and Project Classes

The **Product** and **Project** classes allow easy assignment of a requirement to a product (e.g. *CloudPhoto*) and a project (e.g. *Edition 2019*). Depending on your needs, you may want to create one or both classes.

- **Agile:** Requires the **Product** class
- **Branching:** Requires **Product** and **Project** classes
- **Requirement to Product Assignment:** Requires the **Product** class (without branching)
- **Requirement to Project Assignment:** Requires the **Project** class (without branching)

### Creating Product and Project Classes for Branching

- 1 Start **Class Definition** (see chapter "[Starting Class Definition](#)" on page 270).
- 2 Right-click the canvas, point to Add class on the shortcut menu and select **Product**.
- 3 Click at a free space of the canvas. This adds the **Product** class.
- 4 Change the name to match your needs (e.g. *Products*) and press **Enter**.
- 5 Right-click the canvas, point to Add class on the shortcut menu and select **Project**.
- 6 Click at a free space of the canvas. This adds the **Project** class.
- 7 Change the name to match your needs (e.g. *Projects*) and press **Enter**.
- 8 Save the instance schema.

### Creating Product or Project Classes without Branching

- 1 Start the **Class Definition** tool (see chapter "[Starting Class Definition](#)" on page 270).

- 2 **To create the Product class:**
  - a Right-click the canvas, point to Add class on the shortcut menu and select **Product**.
  - b Click at a free space of the canvas. This adds the **Product** class.
  - c Change the name to match your needs (e.g. *Products*) and press **Enter**.
  - d Continue with point 4.
- 3 **To create the Project class:**
  - a Right-click the canvas, point to Add class on the shortcut menu and select **Project**.
  - b Click at a free space of the canvas. This adds the **Project** class.
  - c Change the name to match your needs (e.g. *Projects*) and press **Enter**.
- 4 If you do not plan to use branching at a later time, you can do the following modifications, so the short name is not required when creating a product or project:
  - a Double-click the class you just created (*Products* or *Projects*). This opens the **Definition of class** dialog.
  - b Double-click the **Short Name** attribute. This opens the **Definition of attribute 'Short Name'** dialog.
  - c Clear the following options:
    - **Attribute Mandatory**
    - **Display For Entry**
  - d Click **OK** to close the **Definition of attribute 'Short Name'** dialog.
  - e Click **OK** to close the **Definition of class** dialog.
- 5 Save the instance schema.

## Supporting Comments

### Overview

Comments can be added to chapters or requirements. Comments allow to discuss topics regarding a requirement or chapter. Rather than just discussing the topics by e-mail or personally, this allows to review all comments at any time, e.g. during an approval process.




**NOTE** To add a comment or reply to a comment, users must have the following permissions:

- **Create** permission on the Comment class
- **Read** permission on the requirement class
- **Create** permission on the relationship between the Comment class and the requirement class.

## Adding the Comment Class and Relationships


The following steps describe how to add the Comment class and to create the relationships with the classes for which you want to support comments. You are free to change the name the Comment class in your schema.

### Execute the following steps:

- 1 In **Class Definition**, do one of the following:
  - Click the **Add Class** button  in the toolbar and select **Comment** from the drop-down.
  - Right-click a blank area of the canvas, point to **Add Class** and select **Comment** from the shortcut menu.
- 2 Move the cursor to where you want to place the class and click the left mouse button. The class symbol is displayed on the diagram and the title is highlighted for editing.
- 3 If desired, change the name **Comment** to a name of your liking.




**CAUTION!** The class name must follow the conventions specified in chapter "Naming Conventions for Class Names" on page 28

- 4 Press **Enter** or click a blank area of the canvas to save the new name.
- 5 Do the following for each class you want to use comments with:
  - a Click the **Add Relationship** button  in the toolbar or right-click a blank area of the canvas and select **Add Relationship**.
  - b Select the class you want to use comments with. This starts the relationship.
  - c Select the *Comment* class. This creates the relationship and highlights the relationship name. Enter a unique name for the relationship which describes the data which will be held in the relationship.
  - d Press **Enter** or click on a blank area of the canvas to commit the new name.



**CAUTION!** The relationship name must follow the conventions specified in chapter "Naming Conventions for Relationship Names" on page 29.

- e Double-click the relationship (the arrow pointing from your class to the *Comment* class). This opens the **Definition of relationship** dialog.
  - f Select the **Constraints** tab.
  - g Ensure, that for **Primary Links** and **Secondary Links**, the option **transfer to child** is selected.
  - h Click **OK**.
- 6 Save the class definition by clicking  in the toolbar or by selecting **Save** from the **File** menu.



## Chapter 10

---

# Configuring Tomcat

Working with Secure Socket Layers	352
Configuring Secure Cookies	367
Restricting Server.xml User Access	369
Configuring HTTP Strict Transport Security and Anti-Clickjacking	369
Configuring the Tomcat Service	370
Removing the Certificate Update Menu	370

## Working with Secure Socket Layers

Secure Socket Layers (SSL) is standard technology for securing an Internet connection by encrypting data sent between a website and a browser (or between two servers). Transport Layer Security (TLS) an updated and more secure version of SSL is recommended for preventing hackers from seeing or stealing information as users communicated with the RM Server.

We recommend that administrators use secure protocols, and use HTTPS to secure Production environments; this is also true for test environments if the same passwords and/or data is used.

### Configuration Overview

When using TLS (or SSL) with Dimensions RM, the certificate of the web server in PFX and CER format must be installed on the RM Server. Certificates are still referred to as SSL Certificates.

For details on importing the certificate to IIS, see chapter ["Importing a PFX Certificate into Microsoft IIS" on page 430](#).

If you are not using IIS, see chapter ["Importing a PFX Certificate into Windows" on page 430](#).



#### 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 PFX Format from the Management Console" on page 434 or
- "Exporting Certificates to CER Format from IIS" on page 433.
- **PFX Format:**
  - "Exporting Certificates to PFX Format from the Management Console" on page 434 or
  - "Exporting Certificates to PFX Format from IIS" on page 435.



**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 439.

**To import the certificate, do the following:**

- 1 Stop the **Dimensions RM 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 **Dimensions RM 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\Open Text\Dimensions 25.2`.
- Replace *###.#* with the Common Tools version number, e.g. `2.3.0.0`
- Replace *##* with the Java version number, e.g. `11.0`.

The complete set command may look like this:

```
set path=%path%;"C:\Program Files\Open Text\Dimensions  
25.2\Common Tools 2.5.0.0\jre\11.0\bin"
```

- 4 If Dimensions RM 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\Open Text\Dimensions 25.2 (13)`.
- Replace *###.#* with the Common Tools version number, e.g. 2.5.0.0.
- Replace *##* with the Tomcat version number, e.g. 10.1.

A complete path may look like this:

```
C:\Program Files\Open Text\Dimensions 25.2\
Common Tools 2.5.0.0\tomcat\10.1\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 439.
- 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\11.0\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 "[Modifying the Server.xml File](#)" on page 356.
- 14 Ensure that the **Dimensions RM Common Tomcat** service is running.

## Modifying the Server.xml File

The server.xml file is a configuration file for Dimensions RM 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 **Dimensions RM 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 **Dimensions RM 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\Open Text\Dimensions 25.2`.
- Replace `#.#.#.#` with the Common Tools version number, e.g. `2.5.0.0`.
- Replace `#.#` with the Tomcat version number, e.g. `10.1`.

A complete path may look like this:

```
C:\Program Files\Open Text\Dimensions 25.2\
Common Tools 2.5.0.0\tomcat\10.1\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"
relaxedQueryChars="[,]"
clientAuth="false" />
```

- 6 Ensure that both connectors are **not surrounded** with `<!--` and `-->`.
- 7 Save the file.
- 8 Start the 'Dimensions RM 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 **Dimensions RM Common Tomcat**.
  - c Click  .
- 9 After Dimensions RM Common Tomcat has been started, Dimensions RM should be available using 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 432](#)  
or
  - ["Exporting Certificates to CER Format from IIS" on page 433](#).
- **PFX Format:**
  - ["Exporting Certificates to PFX Format from the Management Console" on page 434](#)  
or
  - ["Exporting Certificates to PFX Format from IIS" on page 435](#).



**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 439](#).

**To update the certificate, do the following:**

- 1 Stop the **Dimensions RM 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 **Dimensions RM Common Tomcat**.
  - c Right-click and select **Stop**.
- 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\Open Text\Dimensions 25.2\`.
- Replace `###.#` with the Common Tools version number, e.g. `2.5.0.0`.
- Replace `##` with the Java version number, e.g. `11.0`.

The complete set command may look like this:

```
set path=%path%;"C:\Program Files\Open Text\Dimensions 25.2\
Common Tools 2.5.0.0\jre\11.0\bin"
```

- 4 If Dimensions RM 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\Open Text\Dimensions 25.2\`.
- Replace `###.#` with the Common Tools version number, e.g. `2.5.0.0`.
- Replace `##` with the Tomcat version number, e.g. `10.1`.

A complete path may look like this:

```
C:\Program Files\Open Text\Dimensions 25.2\
Common Tools 2.5.0.0\tomcat\10.1\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" relaxedQueryChars="[,]"
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\Open Text\Dimensions 25.2\Common Tools 2.5.0.0\tomcat\10.1\). 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\Open Text\Dimensions
25.2\Common Tools 2.5.0.0\jre\11.0\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 439](#).
- 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\11.0\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 **Dimensions RM 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 **Dimensions RM Common Tomcat**.
  - c Click 

### Updating SSO Certificates

When using Single Sign On (SSO), it may be required to update the certificates in Dimensions RM 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 **Dimensions RM 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 **Dimensions RM 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\Open Text\Dimensions 25.2*.
- Replace *#.#.#.#* with the Common Tools version number, e.g. *2.5.0.0*.
- Replace *#.#* with the Java version number, e.g. *11.0*.

The complete set command may look like this:

```
set path=%path%;"C:\Program Files\Open Text\Dimensions
25.2\Common Tools 2.5.0.0\jre\11.0\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\Open Text\Dimensions 25.2.`
- Replace *###.#* with the Common Tools version number, e.g. 2.5.0.0.
- Replace *##* with the Tomcat version number, e.g. 10.1.

A complete path may look like this:

```
C:\Program Files\Open Text\Dimensions 25.2\
Common Tools 2.5.0.0\tomcat\10.1\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 **Dimensions RM 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 **Dimensions RM 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

Dimensions RM is installed, by default, with the following configuration settings. These settings will require secure https protocol only:

**Secure Cookies:** Prevents data stored in cookies to be retrieved by an attacker.

**HTTP Strict Transport Security and Anti-Clickjacking:** Prevents external websites from overlaying Dimensions RM elements thus ensuring that if a user clicks on a Dimensions RM button the click cannot be caught.

Additionally, the following security headers have been enabled:

- Header to block content type sniffing: `blockContentTypeSniffingEnabled`  
`<param-value>true</param-value>`
- Content-Security-Policy HTTP header: `contentSecurityPolicy`  
`<param-value>frame-ancestors 'self'; form-action 'self';`  
`default-src 'self' 'unsafe-inline' 'unsafe-eval' data:`  
`blob:;</param-value>`

- Referrer-Policy HTTP header  
`<param-value>no-referrer</param-value>`

Should it be necessary to run Dimensions RM over **insecure HTTP**, please refer to

- ["Settings Previously Made at Installation" on page 368](#)
- ["Running Application Load Balancer over Insecure HTTP" on page 368](#)

### **Settings Previously Made at Installation**

In Dimensions RM Releases prior to 24.4 (12.12.1), Secure Cookies and HTTP Strict Transport Security were implemented by the Dimensions RM System Administrator in the Tomcat ...\\conf\\web.xml file.

To configure these to run over HTTP:

- 1** Stop the **Dimensions RM Common Tomcat** service.
- 2** Open `<RM_Installdir>\\Dimensions 25.2\\Common Tools 2.5.0.0\\tomcat\\10.1\\webapps\\rtmBrowser\\WEB-INF\\web.xml` with a text editor, e.g. Notepad.
- 3** Secure Flag for cookies should be set to false:  
`<cookie-config>  
 <secure>false</secure>  
</cookie-config>`
- 4** HTTP Strict Transport Security header should be set to false:  
`<init-param>  
 <param-name>hstsEnabled</param-name>  
 <param-value>>false</param-value>  
</init-param>`
- 5** Save the file.
- 6** Start the **Dimensions RM Common Tomcat** service.
- 7** There is no need to include or to maintain modifications made in previous releases.

### **Running Application Load Balancer over Insecure HTTP**

To address changes made to strengthen Dimensions RM security we have added a new parameter to `<RM_Installdir>\\Dimensions 25.2\\Common Tools 2.5.0.0\\tomcat\\10.1\\webapps\\rtmBrowser\\WEB-INF\\web.xml`.

This parameter will allow users to configure an Application Load Balancer to run over insecure HTTP. To implement, please make the following changes:

- 1** Stop the **Dimensions RM Common Tomcat** service.
- 2** Open `<RM_Installdir>\\Dimensions 25.2\\Common Tools 2.5.0.0\\tomcat\\10.1\\webapps\\rtmBrowser\\WEB-INF\\web.xml` with a text editor, e.g. Notepad.
- 3** Set Flag for `ALBWithInternalNonHTTPsInUse` to true:  
`<!-- Set value to true when Application Load Balancer is used and  
connects to RM server internally by insecure port-->  
<context-param>`

```
<param-name>ALBWithInternalNonHTTPsInUse</param-name>  
<param-value>>true</param-value>  
</context-param>
```

- 4 Save the file.
- 5 Start the **Dimensions RM Common Tomcat** service.

## Configuring HTTP Strict Transport Security and Anti-Clickjacking

Anti-Clickjacking prevents external websites from overlaying Dimensions RM elements thus ensuring that if a user clicks on a Dimensions RM button, for example, the click cannot be caught.

In Dimensions RM Releases **prior** to 24.4 (12.12.1), HTTP Strict Transport Security was implemented by the Dimensions RM System Administrator in the tomcat\9.0\conf\web.xml file.

There is no need to include or to maintain modifications made in previous releases.

Should it be necessary to run Dimensions RM over **insecure HTTP**, please see ["Configuring Secure Cookies" on page 367](#).

## Restricting Server.xml User Access

### RMSERVICEUSER

For increased security, Dimensions RM creates the launching user, RMSERVICEUSER, at installation.

The RMSERVICEUSER does not belong to the Administrators' group, and has no remove login access. The launching user has the necessary permissions to run RM Services following installation.

Reset Password must be used should the Administrator choose to change the RMSERVICEUSER password.

### To restrict user access to the server.xml file, do the following:

The server.xml should be readable only by the RMSERVICEUSER, to restrict access, please do the following.

- 1 Go to <RM Install Dir>\Dimensions 25.2\Common Tools 2.5.0.0\tomcat\10.1\conf
- 2 Right mouse click server.xml, choose Properties
- 3 Select the Security tab.
- 4 In the Advanced Security Settings dialog, select Users Group.
- 5 Click **Disable Inheritance** button.

- 6 In the prompt click **Convert inherited permissions into explicit permissions**.
- 7 Select Users group again and click the Edit button.
- 8 Deselect "Read" and "Read & Execute" permission.
- 9 Click Apply, Click OK, in opened dialogs.
- 10 Start the **Dimensions RM Common Tomcat** service.

## Configuring the Tomcat Service

### 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 x,x\tomcat\10.1\bin*
- 2 Create a copy of the file tomcat9w.exe.
- 3 Rename the copy to opentextTomcatw.exe.

## Removing the Certificate Update Menu

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

- 1 Stop the **Dimensions RM Common Tomcat** service.

Note that users will not be able to work with Dimensions RM or any other web application on the same Tomcat server while you are making changes.

- 2 In Windows Explorer, navigate to the following path:  
Assuming Install directory: *C:\Program Files\Open Text\Dimensions 24.2*

Proceed to:

*\Common Tools 2.5.0.0\tomcat\10.1\webapps\rtmBrowser\rm\frame\panels\top*

- 3 Open the file toppanel.jsp with Notepad.

- 4 Locate the following text:

```
<c:if test="{userDetails.admin}">
    <sct:subMenuItem id="certificateUpdate"
href="javascript:SERENA.rm.settings.certificateUpdate.showDialog();">
        <fmt:message key="RM_CertUpdate_DlgTitle" />
    </sct:subMenuItem>
</c:if>
```

- 5 Surround the text with **<%--** and **--%>**, so it looks like this:

```
<%-- <c:if test="{userDetails.admin}">
```

```
<sct:subMenuItem id="certificateUpdate"
href="javascript:SERENA.rm.settings.certificateUpdate.showDialog();">
    <fmt:message key="RM_CertUpdate_DlgTitle" />
</sct:subMenuItem>
</c:if> --%>
```

- 6** Save the file.
- 7** In Windows Explorer, navigate to the following path:  
*RM\_Install*\Common Tools 2.5.0.0\tomcat\10.1\work
- 8** Delete the Catalina folder.
- 9** Start the **Dimensions RM Common Tomcat** service.



# Chapter 11

---

## RM Import

RM Import Overview	374
Logging in to RM Import	375
Input File Format Dialog	377
Word Import	378
Preview Dialog	380
Draft Requirements Document Import	383
Excel Import	383
Configuring RM Import	388

## RM Import Overview

RM Import allows you to import Word documents, Draft Requirement documents and Excel spreadsheets. For Word documents, import templates are required. These templates can be created with RM Import Designer. For further information on how to create templates, see chapter "RM Import Designer" on page 399.



### IMPORTANT!

- Word uses unique, proprietary styles and formatting; therefore, the styles and formatting of the Word document (for example, lists, bullets, and fonts) are not necessarily preserved in Document View. However, the text is always imported, so there is no data loss.
- You cannot import the changes you make in Document View back into the original Word document. Roundtripping between Dimensions RM and Word is not supported.
- Documents in Document View are *not* the same as the Word documents from which they were imported. Dimensions RM does *not* store the Word document; it parses the data into classes (requirements and so on) so the data is available to the entire instance.
- Users can optionally import directly using RM Browser, without having to first design an import template. Please see the *Dimensions RM Browser User's Guide* for more on importing using the RM Browser client.
- If the machine running RM Import has been configured with limited permissions, import of Word documents is not supported. This kind of configuration is usually made on servers only, not on client machines.

### Note the following:

- Everything in the Word document up to the first heading, except for the Table of Contents, becomes the document description. The document description is captured as an HTML-enabled attribute and can include tables, images, and so on.
- Chapters are automatically captured based on Word headings.
- All subheadings become subchapters until and unless they are later identified as requirements.
- RM Import attempts to import the bodies of the chapters that are not identified as requirements into the description of the chapter. This helps ensure that all data from the Word document is captured.
- Chapters do not need to contain any requirements.
- You can import the requirements from the documents into one class or multiple classes. However, each chapter can contain requirements from only one class.
- On the Dimensions RM server, a supported edition of Microsoft Office (32-bit or 64-bit) must be installed to support document export, RM Import and RM Import Designer tools.  
On the client, Word and Excel (32-bit or 64-bit) must be installed to support RM Import.  
For a list of supported Microsoft Office versions, see the platform matrix <https://www.microfocus.com/documentation/dimensions-rm/>.

The minimum set of pre-installed Microsoft Office components required for the above tools is:

- Microsoft Office Excel (32-bit or 64-bit).
- Microsoft Office Excel .NET Programmability Support.
- Microsoft Office Word (32-bit or 64-bit).
- Microsoft Office Word .NET Programmability Support.

The following should also be noted:

- A message warns you if you do not have Office installed on your computer.
- For consistent and reproducible use of the document export, 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 32-bit or 64-bit edition of Word 2013, 2016, or 2019 must be installed on the server.
- RM Import needs the PIA (Primary Interop Assembly) that is installed by default. No special permissions are required. Before you use RM Import, be sure that Word is activated (that is, open Word at least once before using RM Import).
- The RM Import installation configures the user to run as an interactive user; no other permissions are required. Make sure that any other program associated with the Word document is activated (for example, if you export a Word document with a .pdf attachment, make sure that Adobe® Reader® is activated on the server).

## Logging in to RM Import

Logging in to RM Import is a two-part process:

- Validating the server
- Logging in to the Dimensions RM instance

The server validation must occur before you can log in to a Dimensions RM instance. If you are using secure socket layers (SSL), which is an advanced security feature, a certificate selection dialog may be displayed during the server validation. The situation in which this dialog is displayed is discussed later in this procedure.

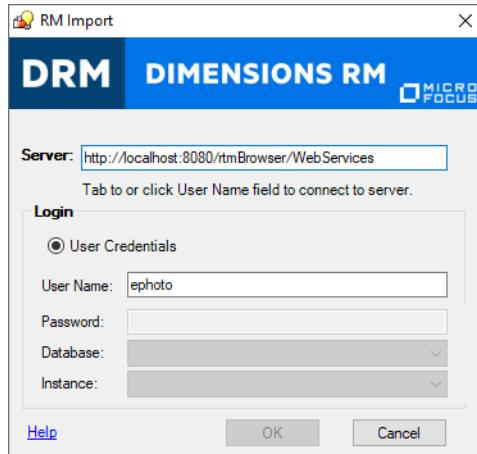


**NOTE** Before you log in, you must know the URL or name and port number (if not 80) of the server running the RM Web service, and have access to at least one instance running on that service.

### To log in to RM Import:

- Do one of the following:
  - Select **Start | Programs | Open Text | Dimensions RM version | RM Import**.
  - Double-click the RM Import shortcut on your desktop.

- The **RM Import login** dialog box opens.



**Figure 11-1. Login Dialog**

- In the **Server** field, type the name of the server that hosts the RM Web service. You can type a full URL or just type the server name and then press the Tab key, and the default URL is built. If the port number is not 80, type the port number after the server name, separated by a colon.

An example URL is `http://PC2040:8080/rtmBrowser/WebServices`



**NOTE** It is a good practice to copy the complete URL that is in the **Server** field to the address bar of a Web browser window and test that it connects to the server on which your Web service is hosted. This is a good test for http and https to validate that the Web service is up and running.

- If your URL includes `https://` for SSL, an additional dialog box can be displayed that lets you choose which personal certificate you want to use. This dialog box is displayed if more than one certificate is in your personal store.



#### NOTES

- This dialog box shows personal certificates only.
- The certificate information is not cached, so you are prompted for a certificate every time you log in.

- The **User Name** field is populated with the last value you entered, if any. If necessary, type your user name.



#### NOTES

- The server connection is attempted when you click on or tab to the **User Name** field.
- The **Password**, **Database**, and **Instance** fields are enabled only after the server is connected.

- In the **Password** field, type your password.
- In the **Database** field, select the Dimensions RM database from which you want to work.

- In the **Instance** field, select the instance with which you want to work.



**NOTE** The instances in the list are those that you have permission to log in to. If no instances appear in the list, then either an error occurred or you do not have permissions for any instance on the server.

- Click **OK**. This opens the Import File Format dialog.

## Command Line RM Import

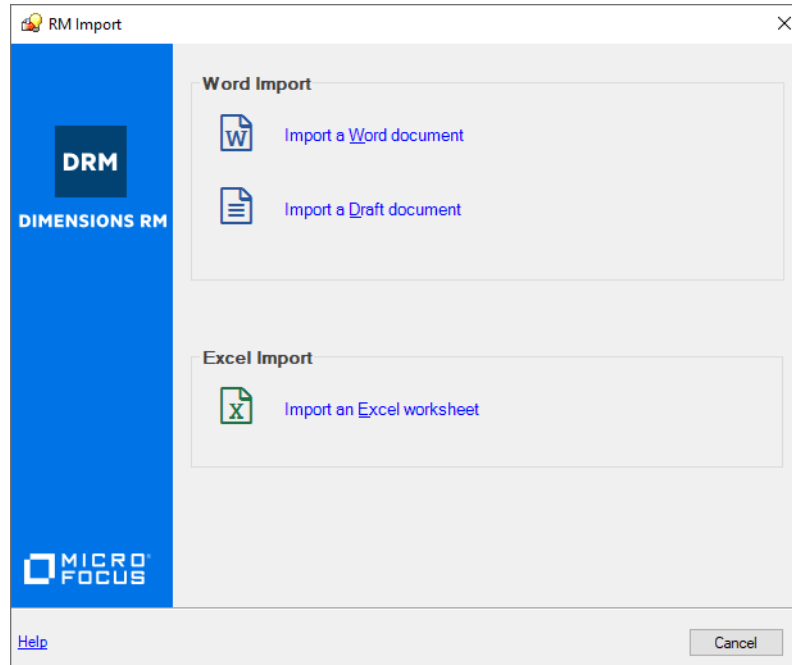
For customers converting from a document based requirements management system to Dimensions RM, it is possible, once the Template has been created using RM Import Designer, to import documents via the command line.

```
RMImport.exe /import /server /Document C:\inputdoc.doc.x /template  
"TDRBasicTemplate" /db mydatabase /proj myinstance /user ImportUser  
/pw UserPassword /output C:\output.log /category RMDemo\Data
```

## Input File Format Dialog

The Import File Format dialog allows you to choose the format of the file to import. These file formats are supported:

- Word Documents (\*.doc, \*.docx, \*.dot or \*.dotx)
- Draft Requirement Documents (\*.drd or \*.xml)
- Excel Spreadsheets (\*.xls or \*.xlsx)



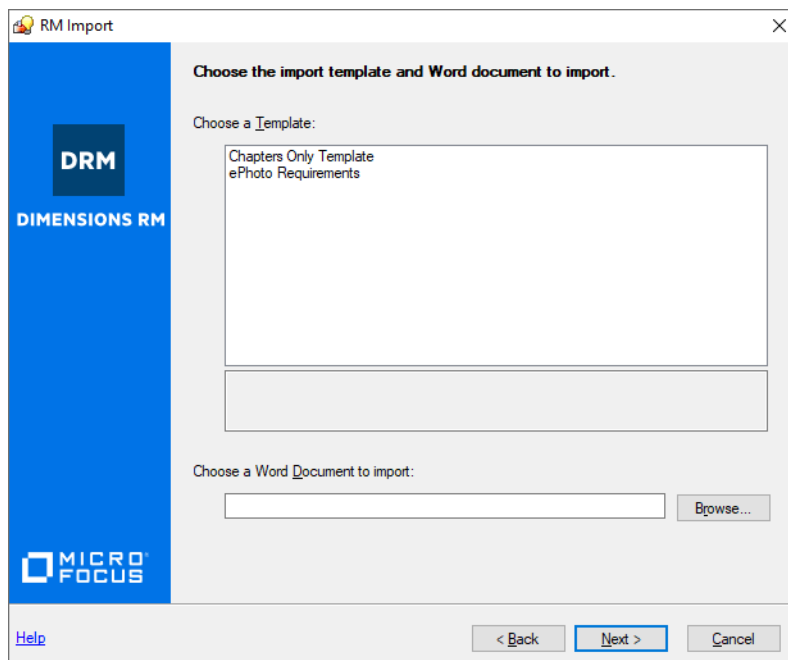
**Figure 11-2. Import File Format Dialog**

**12** Do one of the following:

- To import a Word document, click on **Import Word document**
- To import a Draft Requirement document, click on **Import an existing draft document**
- To import an Excel spreadsheet, click on **Import an Excel sheet**

## Word Import

The Word Import function of RM Import allows you to import Word files with .doc, .docx, .dot and .dotx file extension. RM Import can import the Word document as a whole document or extract requirements from it and store them in Dimensions RM with the classes defined in the template. The following dialog allows you to select a template and a Word document.



**Figure 11-3. Template and Word Document Dialog**

**To complete the Template and Word Document dialog:**

- 1 **Choose a Template list** shows all available templates. Select a template you want to use for import.
- 2 **Choose a Word Document to import** allows you to enter the path to an existing Word document. Alternatively, you can click on **Browse...** to select the Word document through the *Open file* dialog.
- 3 Clicking **Next >** loads the document and shows the preview screen (see chapter "[Preview Dialog](#)" on page 380).
  - Clicking **< Back** returns the import format selection screen.
  - **Cancel** exits RM Import.

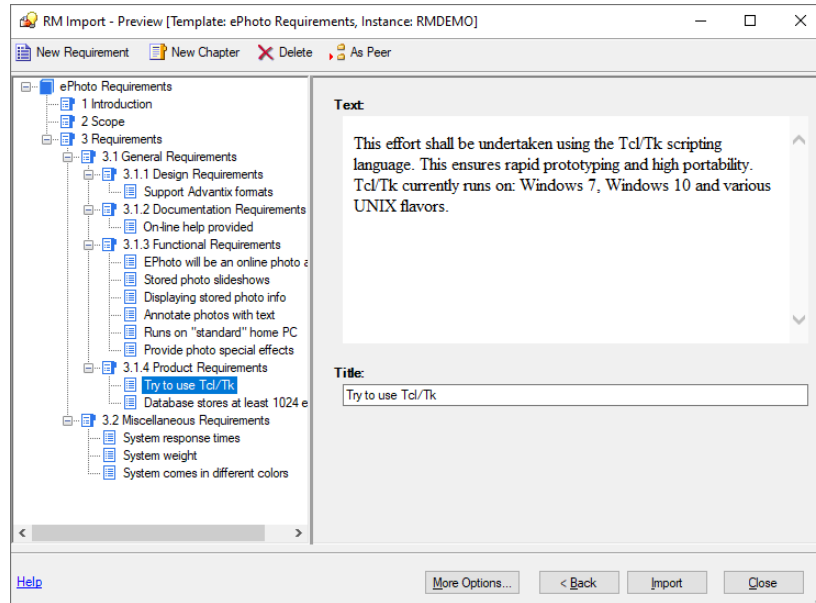
## Date Import Formats

RM Import requires the following:

- The Windows server running the Dimensions RM server needs to use the time zone **(UTC) Coordinated Universal Time**. If a different time zone is used, the dates and times in the imported requirement may differ from those in the document from which they were imported.
- The date specified in a Word document must match the format for the attribute of the requirement class you wish to import.

## Preview Dialog

After parsing the document, RM Import loads it into the **Preview** dialog. Depending on the size of your Word document, the parsing process can take some time. The **Preview** dialog allows to view and to modify the document before uploading it to Dimensions RM.



**Figure 11-4. Preview Dialog**

On the left hand side you find a tree, representing the document chapters and requirements found in the Word document. By using different templates, you might get different parsing results. The document tree uses these icons:



**Document** This icon represents the document which can contain chapters or requirements.



**Chapter** This icon represents a chapter which can contain text, tables or images. A chapter can also contain sub-chapters or requirements.




**Chapter Import OK** This icon shows that the chapter was imported to the Dimensions RM document.





**Chapter Import Error** This icon shows that an error occurred when importing the chapter to the Dimensions RM document.



**Requirement** This icon represents a requirement which can contain text, tables or images. A requirement can also contain sub-requirements.

 **Requirement Import OK** This icon shows that the requirement was imported to Dimensions RM.

 **Requirement Import Error** This icon shows that an error occurred when importing the requirement to Dimensions RM.


 **Resolve Requirement** This icon shows that the requirement has invalid attributes.


The Preview dialog also allows to modify a parsed document before importing it to Dimensions RM. To modify a chapter or requirement, select the desired chapter or requirement in the document tree. To use different formatting it is recommended to edit the text in Microsoft Word and paste it into the document).





**NOTE** The modifications you made are not written to the original Word document.


You can make further modifications by using these functions from the Toolbar:

 **New Requirement** Adds a new requirement to the document. Alternatively, you can add a requirement by right-clicking a chapter or requirement and selecting **New Requirement** from the shortcut menu.

 **New Chapter** Adds a new chapter to the document. Alternatively, you can add a chapter by right-clicking a chapter or requirement and selecting **New Chapter** from the shortcut menu.

 **Delete** Deletes a chapter or requirement from the document. Alternatively, you can delete a chapter or requirement by right-clicking a chapter or requirement and selecting **Delete** from the shortcut menu.

 **As Peer** When adding a chapter or requirement, it is added on the same level as the chapter or requirement which is selected in the document tree.

 **As Child** When adding a chapter or requirement, it is added as a child of the chapter or requirement which is selected in the document tree.

You can access further functions by clicking any of these buttons:

- **More Options** Provides these functions:
  - **View Source** Opens the original Word document.

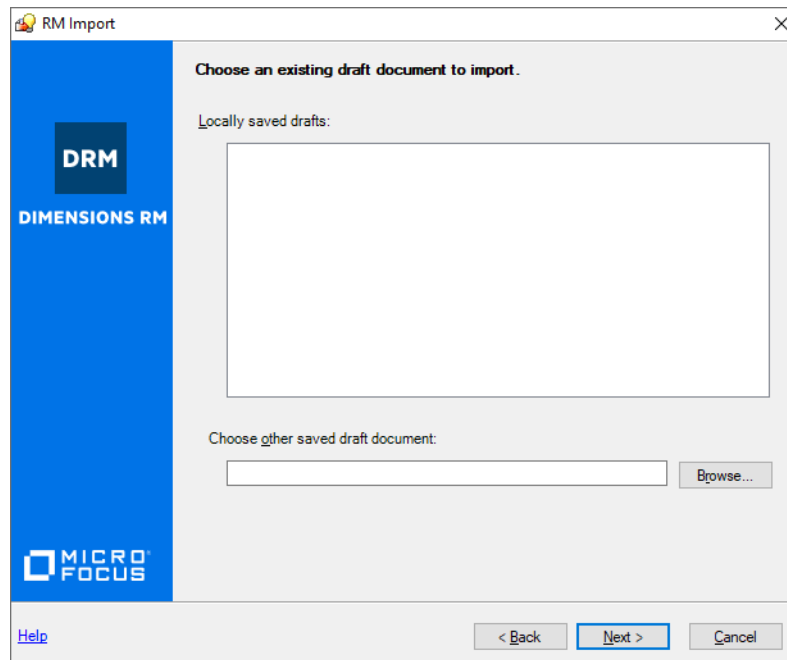
- **Append contents from draft...** Appends the contents of a *Draft Requirements Document* to the current document.
- **Save contents to draft...** Saves the current document as a *Draft Requirements Document*.
- **Import into existing document...** Opens the **Select Document** dialog, which allows you to select an existing Dimensions RM document. Confirming this dialog appends the contents of the current document to the document you selected.
- **About** Opens the **About RM Import** dialog which provides
  - Version number and Copyright
  - Additional information on the home page of Open Text
  - Information about your computer
- **< Back** Returns to the previous dialog (**Select Template and Word Document** or **Select Draft Requirements Document** dialog).
- **Import** Imports the current document to Dimensions RM.
- **Close** Closes RM Import.

To complete the Preview dialog:

- 1 Make the desired modifications
- 2 Click the **Import** button or select **Import into existing document...** after clicking the **More Options...** button

# Draft Requirements Document Import

A **Draft Requirements Document** is a document you created earlier by saving a document from the **Preview** dialog. By using a **Draft Requirements Document** you can continue work at a later time or join two or more documents.



**Figure 11-5. Select Draft Requirements Document Dialog**

## To complete the Select Draft Requirements Document dialog:

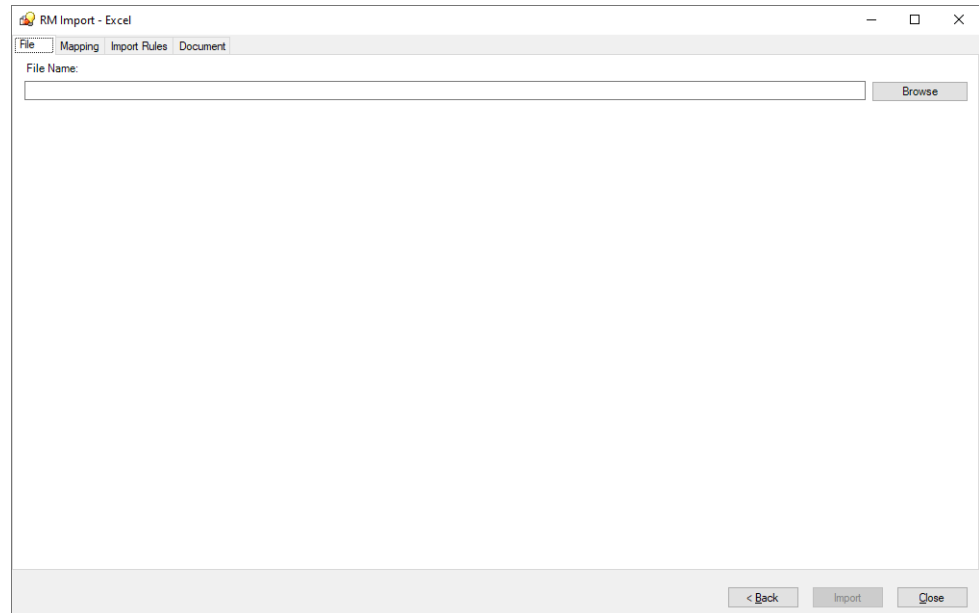
- 1 Select an entry from the **Locally saved drafts** list. Alternatively, you can enter the path to a Draft Requirements Document into the **Choose other saved draft document text box** or click the **Browse...** button and navigate to a Draft Requirement Document.
- 2 Clicking **Next >** loads the document and shows the preview screen (see chapter "Preview Dialog" on page 380).
  - Clicking **< Back** returns the import format selection screen.
  - Clicking **Cancel** exits RM Import.

## Excel Import

The Excel Import function of RM Import allows you to import Excel files with .xls and .xlsx file extension. From an Excel file, RM Import can import requirements and documents. At any time, you can use these functions:

- Clicking **< Back** returns the import format selection screen.
- Clicking **Close** exits RM Import.

## Selecting an Excel File



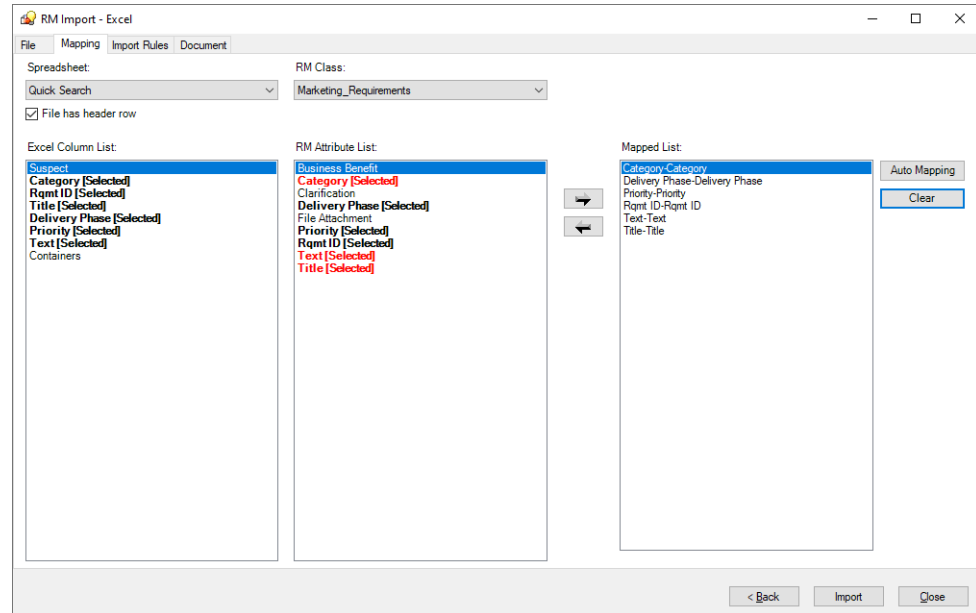
**Figure 11-6. Select Excel File Dialog**

**To select an Excel file, follow these steps:**

- 1** Select the **File** tab.
- 2** Click **Browse**.
- 3** Select the Excel file you wish to import.
- 4** Click **Open**.

## Mapping Excel Columns to RM Attributes

The **Mapping** tab allows you to assign the columns of an Excel worksheet to the associated Dimensions RM attributes. If your Excel file has several worksheets, you can perform the mapping process for multiple worksheets.



**Figure 11-7. Mapping Excel columns to RM Attributes Dialog**

The **Mapping** tab contains these functions:

#### Spreadsheet

The **Spreadsheet** box contains all worksheets of the Excel file.

Select the worksheet you wish to import.

#### RM Class

The **RM Class** box contains all classes of the Dimensions RM server you logged in to.

Select the class into which you wish to import the requirements. If you want to import a document, the class must be a Chapter class.

#### File has header row

The **File has header row** box allows to change between Excel column names (A, B, C ...) and the values of the first row (e.g. Tile, Text, Priority).



#### NOTES

- The **File has header row** box selection is valid for all worksheets. This means that either all worksheets must have header rows or none.
- If the **File has header row** box is selected, the import begins at row 2, skipping the header row.

#### Excel Column List

Contains the columns of the selected worksheet. Columns which have been mapped appear bold and have the suffix **[Selected]**.

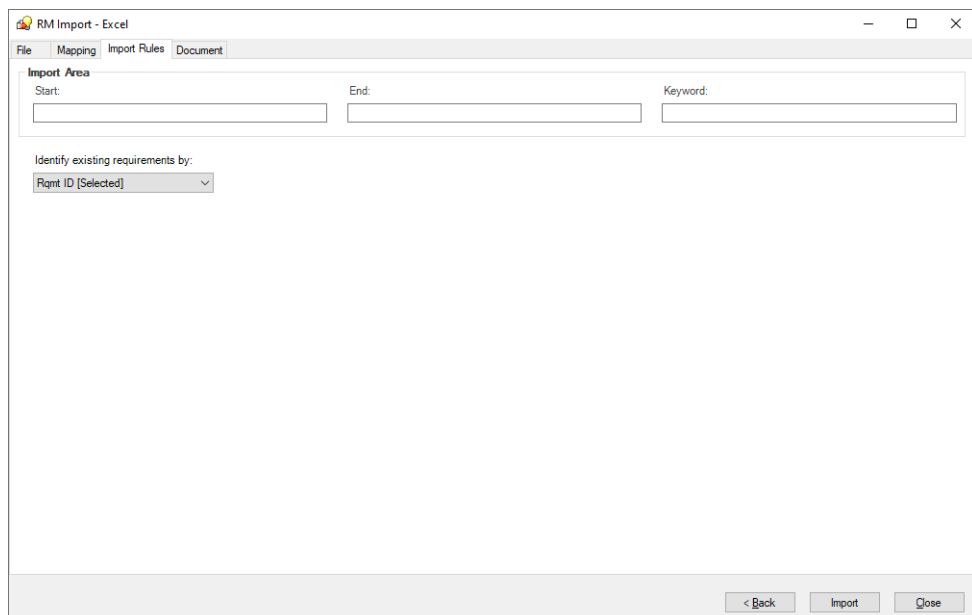
#### RM Attribute List

Contains the attribute names of the selected Dimensions RM class. Attributes that are mandatory, are marked red. Attributes which have been mapped appear bold and have the suffix **[Selected]**.

<b>Mapped List</b>	Contains the mapped Excel columns and attributes.
→	Adds a mapping to the <b>Mapped List</b> box. To add a mapping, select one entry in the <b>Excel Column List</b> box and one entry in the <b>RM Attribute List</b> box.
←	Removes the selected mapping from the <b>Mapped List</b> box.
<b>Auto Mapping</b>	Maps all entries with identical names in <b>Excel Column List</b> box and <b>RM Attribute List</b> box.
<b>Clear</b>	Clears all mappings.

## Configuring Import Rules

The **Import Rules** tab allows you to define where the import should start and end and how to identify requirements to import and how to identify existing requirements. The import rules are defined independently for each mapping.



**Figure 11-8. Import Rules Dialog**

The **Import Rules** tab provides these functions:

### Start



The identifier which defines where to start import. The requirement following the **Start** identifier is the first requirement to be imported.

**TIP** Place the **Start** identifier on a separate line before the first requirement you wish to import.

### End



The identifier which defines where to stop import. The requirement which precedes the **End** identifier is the last requirement to be imported.

**TIP** Place the **End** identifier on a separate line after the last requirement you wish to import.

**Keyword**

The keyword defines which requirement should be imported. Note that RM Import imports the requirement if the keyword is found in any column of that requirement.

**Identify existing requirements by**

By selecting the attribute from the list, RM Import can check if the requirement in the list already exists.

If an attribute is selected, existing requirements will be replaced and nonexisting requirements will be added.

If no attribute is selected, all requirements will be added.

## Configuring Document Settings

The **Document** tab allows to create a new document or to replace an existing document. The document settings are defined independently for each mapping. Note that for importing a document, you need to map a Chapter class.

**Figure 11-9. Document Settings Dialog**

**To import a document, follow these steps:**

- 1** Select the **Import into RM document** box.
- 2** Select **Create Document** and enter a name for the document into the **Name** box to import the requirements into a new document.  
Select **Replace Document** and select a document from the **Name** box to import the requirements into the selected document.
- 3** In the **Sequence Number** box, select the Excel column which contains the sequence number. The sequence number specifies the order in which the requirements should be added to each chapter.
- 4** In the **Chapter Title** box, select the Excel column which contains the chapter title. If you do not select the chapter title, the chapters will not be created.

**In addition, you can do any of the following:**

- Enter a document foreword into the **Description** box.
- In the **Chapter Description** box, select the column which contains the description for the chapter.

## Importing

To import the requirements or documents, click **Import**. The **Import** button is only available if all necessary settings have been made. During import, RM Import shows a progress dialog. Note that the import cannot be canceled once it started. After import is complete, RM Import opens a report to show which requirements or chapters have been imported.

## Configuring RM Import

The administrator can configure RM Import by modifying its configuration file. The configuration file is in the same directory as RM Import and has the name `RmImport.exe.config`. The configuration file is an XML file and thus you can open it with a text editor (e.g. Notepad).

### Configuring the Security Protocol

RM Import supports these protocols for connecting to the web service:

Protocol	Setting
SSL 3	SSL3
TLS 1.0	TLS
TLS 1.1	TLS11
TLS 1.2	TLS12



**NOTE** For TLS 1.1 and TLS 1.2, **.NET 4.5** or higher must be installed on the machine running RM Import.

You can choose any combination of the supported protocols by combining the settings with the pipe symbol, e.g. `SSL3|TLS`.

To configure the security protocol, do the following:

- 1 Open the file `RM_Install\RM\bin\RmImport.exe.config` in a text editor, e.g. Notepad.



**NOTE** Depending on the access rights for the containing directory and operating system configuration, you may have to start the text editor as an administrator and then browse to the file location.

- 2 Locate the following text:  
`<setting name="SecurityProtocol" serializeAs="String">`

- 3 Locate the related **<value>** tag.
- 4 Replace the text between **<value>** and **</value>** with the protocols you want to enable.  
Examples:

Supported Protocols	Setting
SSL 3 and TLS 1.0	SSL3 TLS
TLS 1.0 only	TLS
TLS 1.1 and TLS 1.2	TLS11 TLS12
TLS 1.2 only	TLS12
Any protocol	SSL3 TLS TLS11 TLS12

The security protocol setting should look like this for supporting any protocol:

```
<setting name="SecurityProtocol" serializeAs="String">
<value>SSL3|TLS|TLS11|TLS12</value>
</setting>
```

- 5 Save the file.
- 6 Restart RM Import if it is already running.



# Chapter 12

---

## **WIRIS Editor**

Overview	392
Installing the WIRIS Editor	392
Configuring the WIRIS Editor	392
Configuring Dimensions RM for the WIRIS Editor	395

## Overview

The WIRIS editor allows users to enter mathematical formulas in Dimensions RM. This functionality is only available for text attributes in HTML format, e.g. HTML enabled text attributes in requirements or chapters in documents. I

In order to use this component go to [www.wiris.com](http://www.wiris.com) and download **MathType for TinyMCE 4**.

## Installing the WIRIS Editor

For installing the WIRIS editor server component, you need the `pluginwiris_engine.war` file and the `tiny_mce_wiris` directory, which contains additional directories and files. Both, `pluginwiris_engine.war` and `tiny_mce_wiris`, are part of the **MathType for TinyMCE 4** ZIP archive.

**To install the WIRIS editor, follow these steps:**

- 1 Unarchive the **MathType for TinyMCE 4** ZIP archive.
- 2 Copy the `pluginwiris_engine.war` file into the Tomcat installation webapps directory. For example: `C:\Program Files\Open Text\Dimensions 25.2\Common Tools 2.5.0.0\tomcat\10.1\webapps`
- 3 Check the folder, `webapps\rtmBrowser\rm\vendor\tiny_mce\plugins`  
If this folder contains a `tiny_mce_wiris` directory, **delete** it.
- 4 Copy the `tiny_mce_wiris` directory into `webapps\rtmBrowser\rm\vendor\tiny_mce\plugins`
- 5 Start the Dimensions RM Common Tomcat service.

## Configuring the WIRIS Editor

After installing the WIRIS editor, you need to make some changes to the configuration. The following sections describe how to configure the WIRIS editor and register it with Dimensions RM.

### **Updates to web.xml Settings**

As of Dimensions RM release 24.4 (12.12.1), RM is installed with a secure web.xml configuration.

When installing the WIRIS editor with Dimensions RM release 24.4 or higher or upgrading from any release prior to 24.4, the following changes must be applied.

- 1 Stop the **Dimensions RM Common Tomcat** service.
- 2 Open `<RM Install Dir>\Dimensions 25.2\Common Tools 2.5.0.0\tomcat\10.1\webapps\rtmBrowser\WEB-INF\web.xml`  
with a text editor, e.g. Notepad.

Find param: contentSecurityPolicy and comment the <init-param> tags that contain it. The result is as follows:

```
<!--init-param>
<param-name>contentSecurityPolicy</param-name>
<param-value>frame-ancestors 'self'; form-action 'self'; default-
  src 'self' 'unsafe-inline' 'unsafe-eval' data: blob;;</param-
  value>
</init-param-->
```

- 3 Save the file.
- 4 Start the **Dimensions RM Common Tomcat** service.

### **Configuring the Work Directory**

**To configure the work directory for the WIRIS editor, execute these steps:**

- 1 Start the Registry Editor.
- 2 Navigate to  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Micro Focus\Dimensions RM\Environment\Default.
- 3 Double click the TEMP\_DIRECTORY value. This opens the **Edit String** dialog.
- 4 Ensure that the whole path is selected and press **Ctrl+C** to copy it to the Clipboard.
- 5 Paste the copied path into the address box of Windows Explorer and press **Enter**. This navigates to the path you copied.
- 6 Create a new folder and name it *wiris*.
- 7 In Windows Explorer, navigate to <RM Install Dir>\Dimensions 25.2\Common Tools 2.5.0.0\tomcat\10.1\webapps\pluginwiris\_engine\WEB-INF\pluginwiris.
- 8 Check if the file configuration.ini exists. If it does not exist, rename configuration.ini.dist to configuration.ini.
- 9 Open the file configuration.ini with a text editor, e.g. Notepad.
- 10 Find the variable wiriscachedirectory.
- 11 Remove the # in front of the variable.
- 12 Replace the existing path (following the = sign) with the path you previously copied to the Clipboard.
- 13 Duplicate the backslash characters in the path for the wiriscachedirectory variable, and add \\wiris to the path, so it will look something like this:  
C:\\Program Files\\Open Text\\Dimensions 25.2\\Common Tools 2.4.0.0\\tomcat\\9.0\\webapps\\rtmBrowser\\temp\\wiris.
- 14 Copy the whole path of the wiriscachedirectory variable to the Clipboard.
- 15 Find the variable wirisformuladirectory.
- 16 Remove the # in front of the variable
- 17 Replace the existing path (following the = sign) with the path you previously copied to the Clipboard.

- 18 Save the file.
- 19 Start the Registry Editor.
- 20 Navigate to HKEY\_LOCAL\_MACHINE\SOFTWARE\Micro Focus\Dimensions RM\Environment and select the **Default** registry key.
- 21 Right-click **Default**, point to **New** and then click **String Value**.
- 22 Name the new registry value *WIRIS\_cache\_path*.
- 23 Copy the path you assigned to *wiriscachedirectory* variable to the Clipboard.
- 24 Double-click the registry value *WIRIS\_cache\_path* and paste the path into the **Value data** box.
- 25 Click **OK**.

### **Additional Settings**

#### **To configure additional settings, execute these steps:**

- 1 Start the Registry Editor.
- 2 Navigate to HKEY\_LOCAL\_MACHINE\SOFTWARE\Micro Focus\Dimensions RM\Environment and select the **Default** registry key.
- 3 Right-click **Default**, point to **New** and then click **DWORD (32 bit) Value**.
- 4 Name the new registry value *WIRIS\_max\_retries*.
- 5 Double-click registry value *WIRIS\_max\_retries*.
- 6 Click the **Decimal** option.
- 7 Enter **1200** into the **Value** box. The value specifies the maximal number of attempts for reading the equation picture from the cache.
- 8 Click **OK**.
- 9 In Windows Explorer, navigate to <RM Install Dir>\Dimensions 25.2\Common Tools 2.5.0.0\tomcat\10.1\webapps\pluginwiris\_engine\WEB-INF\pluginwiris.
- 10 Open the file `configuration.ini` with a text editor (e.g. Notepad).
- 11 To configure the save mode:
  - a Find the variable `wiriseditorsavemode`.
  - b Remove the `#` in front of the variable.
  - c Replace the existing value (following the = sign) with **image**, so the line reads:  
`wiriseditorsavemode = image`
- 12 To configure the image format:
  - a Find the variable `wirisimageformat`.
  - b Remove the `#` in front of the variable.



```
],  
  toolbar: [  
    "undo redo | styleselect | bold italic forecolor bgcolor fontselect  
    fontselect | alignleft aligncenter alignright alignjustify | bullist  
    numlist outdent indent | link unlink image fullscreen qpimage mxgraph" +  
    (window.suppressGlossarySupport ? "" : " | glossary") + "  
    tiny_mce_wiris_formulaEditor"],
```

## Configuring the Inline HTML Editor

The following steps describe how to configure the WIRIS editor for the **Entire Document** view (editing chapter descriptions and HTML enabled attributes of requirements).

**To configure the WIRIS editor for requirements and chapters, do the following:**

- 1 Navigate to the <RM Install Dir>\Dimensions 25.2\Common Tools 2.5.0.0\tomcat\10.1\webapps\rtmBrowser\rm\common\js directory and open the file doc-editable.js with a text editor (e.g. Notepad).
- 2 Locate the **tinyMCE.init** function call.
- 3 In the **plugins** section, add tiny\_mce\_wiris to the existing collection if it does not exist (see sample code below).
- 4 In the **toolbar** section, add tiny\_mce\_wiris\_formulaEditor to the existing collection if it does not exist (see sample code below).
- 5 Save the file.

### Sample Code:

```
plugins: [  
  "saveinline image searchreplace print paste fullscreen advlist  
  lists",  
  "noneditable autoresize code textcolor linkext charmap mxgraph" +  
  (rtmDdInitData.glossaryEnabled ? " glossary" : "") + (addTablePlugin ? "  
  table" : "") + " tiny_mce_wiris",  
  "colorpicker pagebreak fields"  
],  
  toolbar: [  
    "(!isObject ? "save cancel | " : "" ) + "bold italic forecolor  
    bgcolor fontselect fontselect "  
    + "alignleft aligncenter alignright alignjustify | bullist numlist  
    outdent indent | openlink "  
    + "link unlink image fullscreen qpimage mxgraph | addcaption  
    addreference "  
    + " tiny_mce_wiris_formulaEditor"  
    + (rtmDdInitData.glossaryEnabled ? " | glossary" : "")
```

```
+ " fields splitText | close",
],
```

## Configuring the Editable Grid

The following steps describe how to configure the WIRIS editor for the editable grid, which can be used in Quick Search, reports and documents.

### To configure the WIRIS editor for the editable grid, do the following:

- 1 Navigate to the <RM Install Dir>\Dimensions 25.2\Common Tools 2.5.0.0\tomcat\10.1\webapps\rtmBrowser\rm\ext\Us directory and open the file TinyMceEditor.js with a text editor (e.g. Notepad).
- 2 Locate the **tinyMCE.init** function call.
- 3 In the **plugins** section, add `tiny_mce_wiris` to the existing collection if it does not exist (see sample code below).
- 4 In the **toolbar** section, add `tiny_mce_wiris_formulaEditor` to the existing collection if it does not exist (see sample code below).
- 5 Save the file.

### Sample Code:

```
plugins: [
    "table image searchreplace print paste fullscreen advlist lists",
    "noneditable autoresize code textcolor linkext charmap mxgraph
glossary tiny_mce_wiris",
    "colorpicker pagebreak close saveinline"
],
toolbar: [
    "undo redo | styleselect | bold italic forecolor backcolor fontselect
fontsize select | alignleft aligncenter alignright alignjustify | bullist
numlist outdent indent | link unlink image fullscreen qpimage mxgraph"
+ " tiny_mce_wiris_formulaEditor"
+ (window.suppressGlossarySupport ? "" : " | glossary | close")
],
```

## Restart Dimensions RM Services

After completing all settings, restart the following services:

- Dimensions RM Common Tomcat
- Dimensions RM Pool Manager



# Chapter 13

---

## RM Import Designer

RM Import Designer Overview	400
Logging in to RM Import Designer	401
Commands	403
General Tab	406
Chapter Rules Tab	407
Requirement Rules Tab	408
Class Rules Tab	412
Preview Tab	424
Word Regular Expressions	425
Limitations	427
Examples	428

## RM Import Designer Overview

RM Import Designer allows you to design templates that users select when importing Microsoft® Word documents into Dimensions RM. Templates define how to identify classes, attributes, chapters, requirements, and categories. Templates can be saved to the database for future use. You must be knowledgeable about class types and the structure of the Word documents that will be imported.

The RM Import tool allows users to preview a Word document, change the description of chapters, reorganize the chapters, change the values of attributes, move attributes between chapters, and so on. When satisfied with the document, users can import it into Dimensions RM as a document that can be viewed and edited from Document View.



### IMPORTANT!

- Word uses unique, proprietary styles and formatting; therefore, the styles and formatting of the Word document (for example, lists, bullets, and fonts) are not necessarily preserved in Document View. However, the text is always imported, so there is no data loss.
- Documents in Document View are *not* the same as the Word documents from which they were imported. Dimensions RM does *not* store the Word document; it parses the data into classes (requirements and so on) so the data is available to the entire instance.
- Users can optionally import directly using RM Browser, without having to first design an import template. Please see the *Dimensions RM Browser User's Guide* for more on importing using the RM Browser client.
- If the machine running RM Import has been configured with limited permissions, import of Word documents is not supported. This kind of configuration is usually made on servers only, not on client machines.

For more information about RM Import, see the chapter "[RM Import](#)" on page 373. For more information about Document View, see the *Dimensions RM Browser User's Guide*.

### Note the following:

- Everything in the Word document up to the first heading, except for the Table of Contents, becomes the document description. The document description is captured as an HTML-enabled attribute and can include tables, images, and so on.
- Chapters are automatically captured based on Word headings.
- All subheadings become subchapters until and unless they are later identified as requirements.
- RM Import attempts to import the bodies of the chapters that are not identified as requirements into the description of the chapter. This helps ensure that all data from the Word document is captured.
- Chapters do not need to contain any requirements.
- You can import the requirements from the documents into one class or multiple classes. However, each chapter can contain requirements from only one class.
- On the Dimensions RM server, a supported edition of Microsoft Office (32-bit or 64-bit) must be installed to support document export, RM Import and RM Import Designer tools.

On the client, Word and Excel (32-bit or 64-bit) must be installed to support RM Import.

For a list of supported Microsoft Office versions, see the platform matrix at <https://www.microfocus.com/documentation/dimensions-rm/>.

The minimum set of pre-installed Microsoft Office components required for the above tools is:

- Microsoft Office Excel (32-bit or 64-bit).
- Microsoft Office Excel .NET Programmability Support.
- Microsoft Office Word (32-bit or 64-bit).
- Microsoft Office Word .NET Programmability Support.

The following should also be noted:

- A message warns you if you do not have Office installed on your computer.
- For consistent and reproducible use of the document export, 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 32-bit or 64-bit edition of Word 2013, 2016, or 2019 must be installed on the server.
- RM Import needs the PIA (Primary Interop Assembly) that is installed by default. No special permissions are required. Before you use RM Import, be sure that Word is activated (that is, open Word at least once before using RM Import).
- The RM Import installation configures the user to run as an interactive user; no other permissions are required. Make sure that any other program associated with the Word document is activated (for example, if you export a Word document with a .pdf attachment, make sure that Adobe® Reader® is activated on the server).



**IMPORTANT!** Before you prepare a template that will be used to import a Word document, save the document as HTML and examine the results. This is the way the document will be displayed in RM Browser after it is imported. If you see any formatting problems that are unacceptable (for example, problems with lists, bullets, and fonts), adjust the styles used in the Word document until the results are satisfactory.



**CAUTION!** If you do not enable the Description attribute for HTML, then formatting and images are not imported. For instructions for enabling the Description attribute for HTML, see "Text Attribute" on page 291.

## Logging in to RM Import Designer

Logging in to RM Import Designer is a two-part process:

- Validating the server
- Logging in to the Dimensions RM instance

The server validation must occur before you can log in to a Dimensions RM instance. If you are using secure socket layers (SSL), which is an advanced security feature, a certificate selection dialog may be displayed during the server validation. The situation in which this dialog is displayed is discussed later in this procedure.

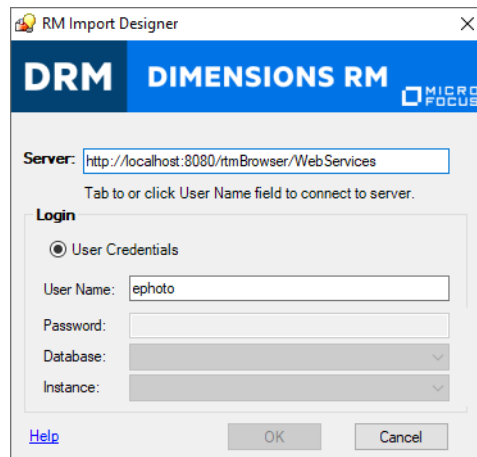


**NOTE** Before you log in, you must know the URL or name and port number (if not 80) of the server running the RM Web service, and have access to at least one instance running on that service.

### To log in to RM Import Designer:

- 1 Do one of the following:
  - Select **Start | Programs | Open Text | Dimensions RM version | RM Import Designer**.
  - Double-click the RM Import Designer shortcut on your desktop.

The **RM Import Designer login** dialog box opens.



**Figure 13-1. Login Dialog**

- 2 In the **Server** field, type the name of the server that hosts the RM Web service. You can type a full URL or just type the server name and then press the Tab key, and the default URL is built. If the port number is not 80, type the port number after the server name, separated by a colon.

An example URL is `http://PC2040:8080/rmBrowser/WebServices`



**NOTE** It is a good practice to copy the complete URL that is in the **Server** field to the address bar of a Web browser window and test that it connects to the server on which your Web service is hosted. This is a good test for http and https to validate that the Web service is up and running.

If your URL includes `https://` for SSL, an additional dialog box can be displayed that lets you choose which personal certificate you want to use. This dialog box is displayed if more than one certificate is in your personal store.



#### NOTES

- This dialog box shows personal certificates only.
- The certificate information is not cached, so you are prompted for a certificate every time you log in.

- 3 The **User Name** field is populated with the last value you entered, if any. If necessary, type your user name.



#### NOTES

- The server connection is attempted when you click on or tab to the **User Name** field.
- The **Password**, **Database**, and **Instance** fields are enabled only after the server is connected.

- 4 In the **Password** field, type your password.
- 5 In the **Database** field, select the Dimensions RM database from which you want to work.
- 6 In the **Instance** field, select the instance with which you want to work.



**NOTE** The instances in the list are those that you have permission to log in to. If no instances appear in the list, then either an error occurred or you do not have permissions for any instance on the server.

- 7 Click **OK**. The **RM Import Designer** window opens to the **General** tab.

## Commands

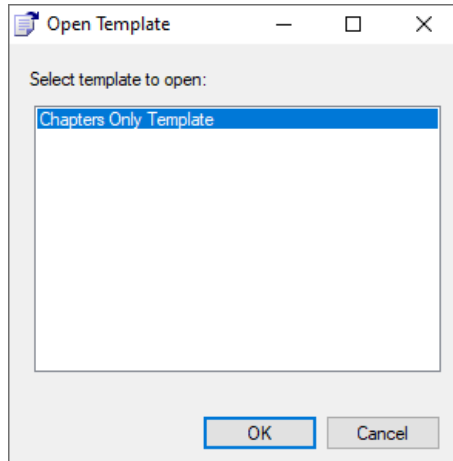
The following sections describe how to perform the commands that are available on the RM Import Designer toolbar.

### Opening an Existing Template

**To open an existing template:**

- 1 Click **Open** on the RM Import Designer toolbar.

The **Open Template** dialog box opens.



**Figure 13-2. Open Template**

- 2 Select the template you want to open and click **OK**.

## Creating a New Template

**To create a new template:**

- 1 Click **New** on the RM Import Designer toolbar.  
The number of the template in the title bar and in the **Name** field is incremented by one.
- 2 Complete the tabs in RM Import Designer as described in this chapter.
- 3 Click **Save** on the RM Import Designer toolbar.

## Saving a Template

**To save a template:**

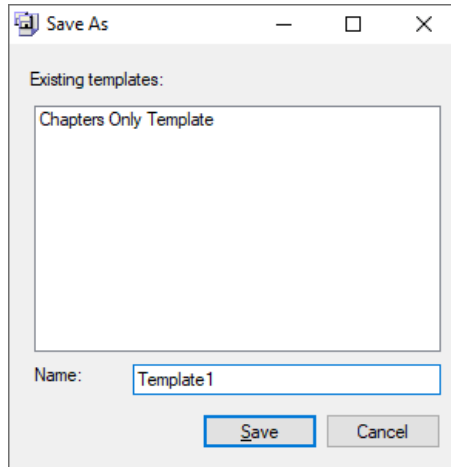
- Click the **Save** button on the RM Import Designer toolbar.

## Saving a Template with Another Name

**To save a template with another name:**

- 1 Click **Save As** on the RM Import Designer toolbar.

The **Save As** dialog opens.



**Figure 13-3. Save As**

- 2 To save this template with another name, type the name in the **Name** field.
- 3 Click **Save**.

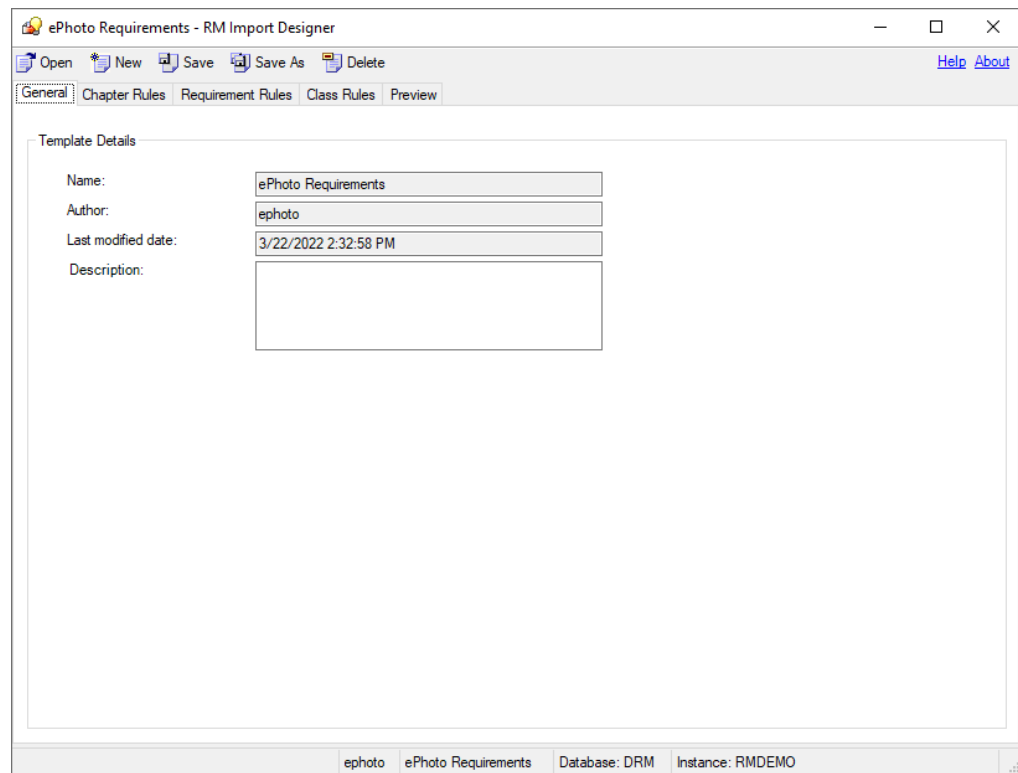
## Deleting a Template

### To delete a template:

- 1 Open the template you want to delete.
- 2 Click **Delete** on the RM Import Designer toolbar.
- 3 Confirm the deletion in the confirmation dialog box that opens.

## General Tab

After you log in to RM Import Designer, the **RM Import Designer** dialog box opens to the **General** tab.



**Figure 13-4. General Tab**

### To complete the General tab:

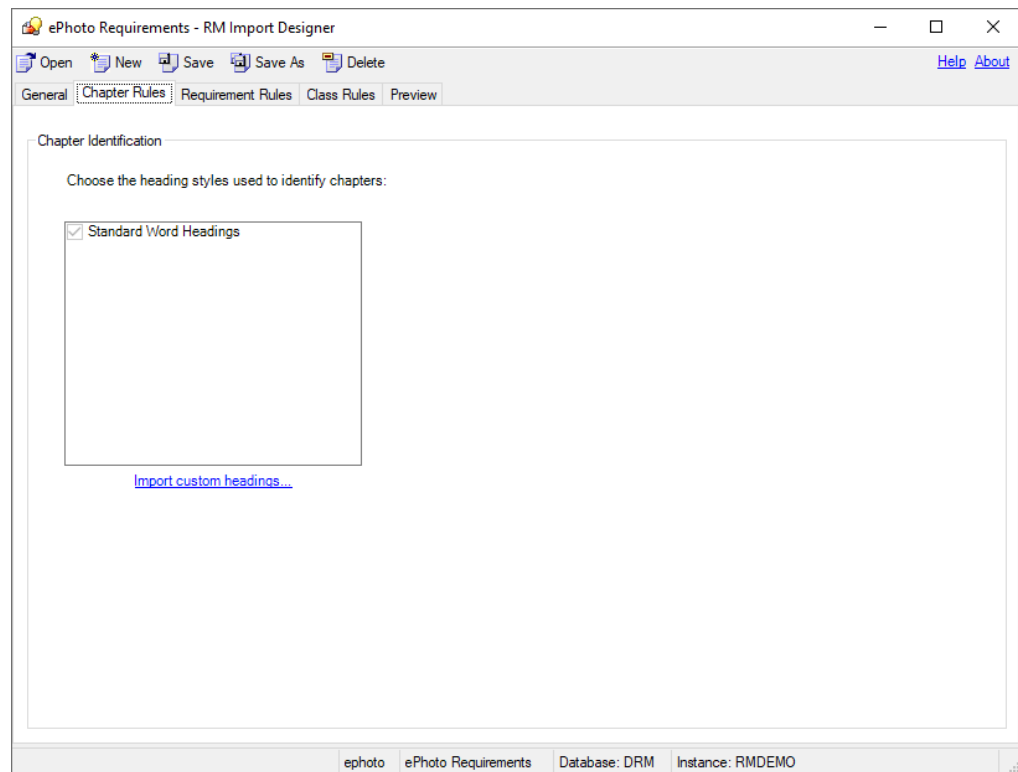
- 1 **Name** is a read-only field that contains the name of the template. When you create the template, the name is Template<*n*>, where <*n*> is the next numbered template. You can change the name by clicking **Save As** and typing a new file name.
- 2 **Author** is a read-only field that contains the user name of the person who created the template. If this is a new template, this field contains the user name of the person who just logged in to RM Import Designer.
- 3 **Last modified date** is a read-only field that contains the date and time that the template was created or saved. For a template that has not yet been saved, this field contains the date and time that the user logged in.
- 4 In the **Description** field, type an optional description of the template. Any description you type in this field is displayed in import mode, and helps the user determine which template to select for the import.

# Chapter Rules Tab

The **Chapter Rules** tab gives you choices for identifying chapters. Chapters are captured automatically according to Word headings, similar to the way Word builds a table of contents. The automatic capture of headings as chapters helps maintain the structure and organization of documents.



**NOTE** By default, all headings are captured as chapters. If the requirement rules identify these headings as requirements, then the requirement rules take precedence and the headings and subheadings are identified as requirements.



**Figure 13-5. Chapter Rules Tab**



**NOTE** If the document you are importing uses custom headings (headings other than the standard nine Word headings), you can load the headings from the document and select the ones you want to use in the document. The same list of custom headings are presented on the **Requirement Rules** tab.

### To complete the Chapter Rules tab:

- 1 If you want to use custom heading styles in addition to standard Word headings to identify the beginning of a chapter in a document, click **Import custom headings**. The **Open** dialog box opens.
- 2 Type or browse to the Word document from which you want to load heading styles, and click **Open**.  
The custom headings from the document are displayed in the list box.
- 3 Select the custom headings that you want to use to identify chapters.

## Requirement Rules Tab

The **Requirement Rules** tab is used to identify the requirements in the document, and varies depending on the option you select under **Requirement Identification**. Each option presents a pattern in which requirements can be identified. The option you select affects the attribute patterns available on the **Class Rules** tab.

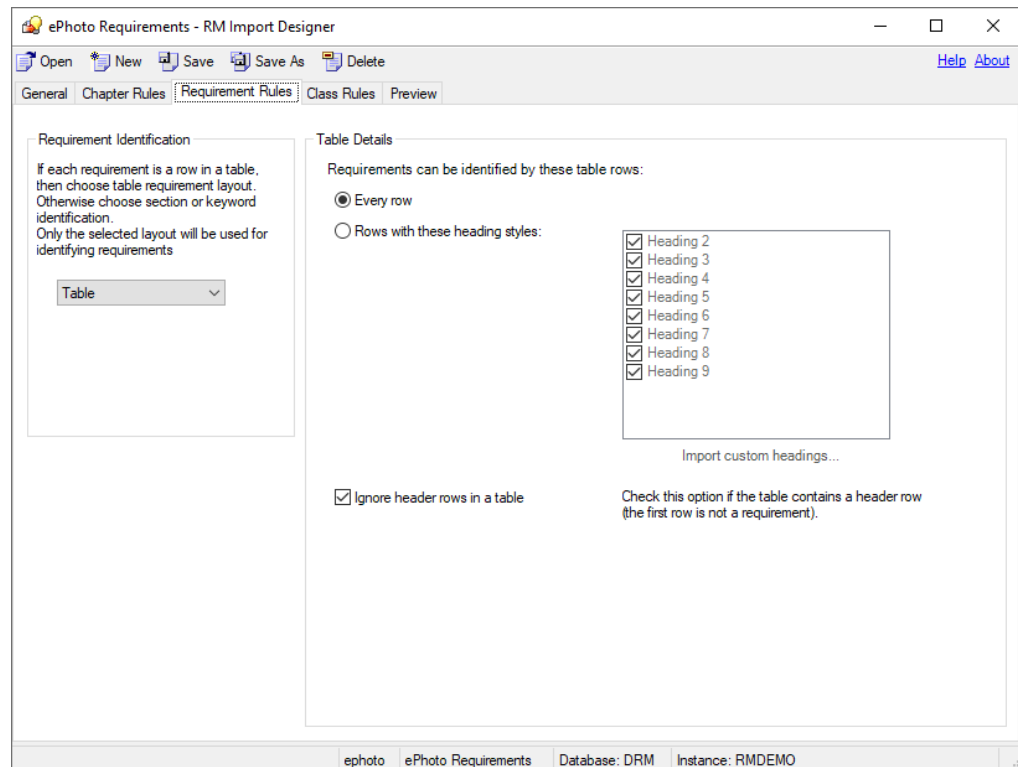


### NOTES

- You can use the **Preview** tab to see how each option affects the import.
- A red exclamation mark indicates that a mandatory default value must be specified.

## Table Option

The choices presented with the **Table** option allow you to distinguish rows in tables that contain requirements from those that do not. Use the **Table** option if requirements are in table rows.



**Figure 13-6. Requirement Rules Tab—Table Layout**

**To complete the Requirement Rules tab for the Table option:**

- 1 Under **Requirement Identification**, select **Table**.

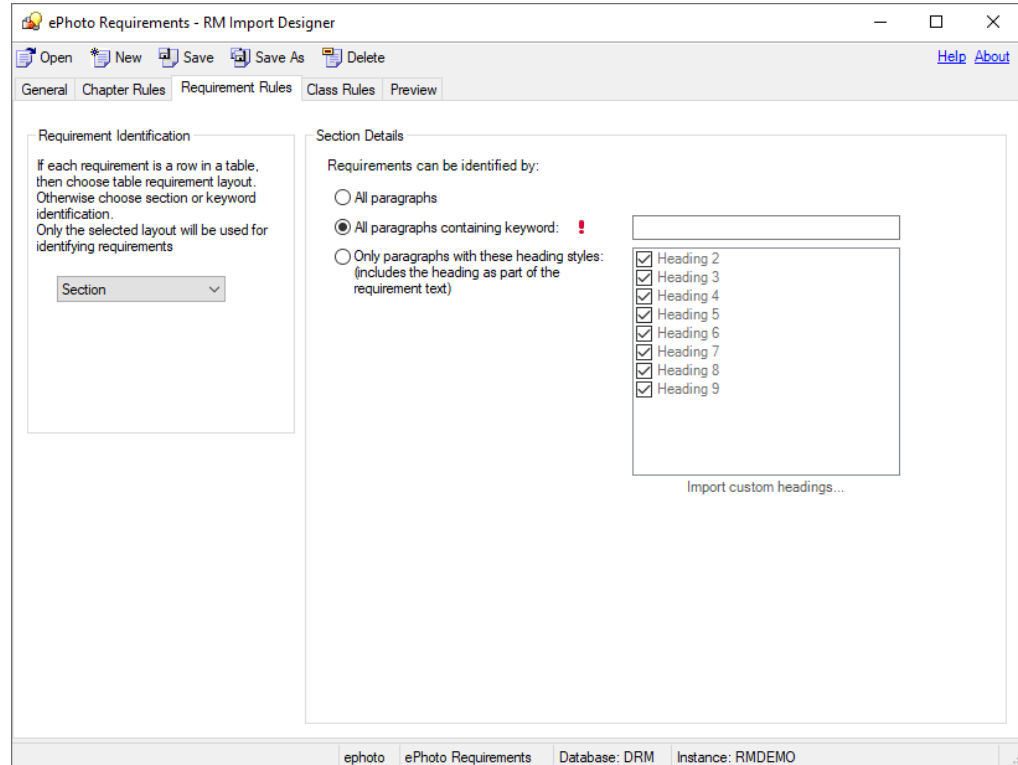
- 2 Under **Table Details**, select one of the options described in the following table.

Option	Description
Every row	Select this option for documents in which all tables contain requirements.
Rows with these heading styles	Select this option when a requirement is in a table with a table cell containing a standard Word heading style. Tables that do not contain a heading are not identified as containing requirements and become part of the chapter description. If you want to use custom headings, click <b>Import custom headings</b> , and type to or browse to the Word document from which you want to load custom styles. Select those headings that you want to use to identify requirements. <b>NOTE:</b> If you imported custom headings on the <b>Chapter Rules</b> tab, this list is automatically populated with the headings from the document you specified there.

- 3 Select the **Ignore header rows in a table** check box if the table contains a header row (that is, the first row in the table contains the names of columns and not a requirement).

## Section Option

Use the **Section** option to identify sections of the Word document that contain requirements.



**Figure 13-7. Requirement Tab—Section Option**

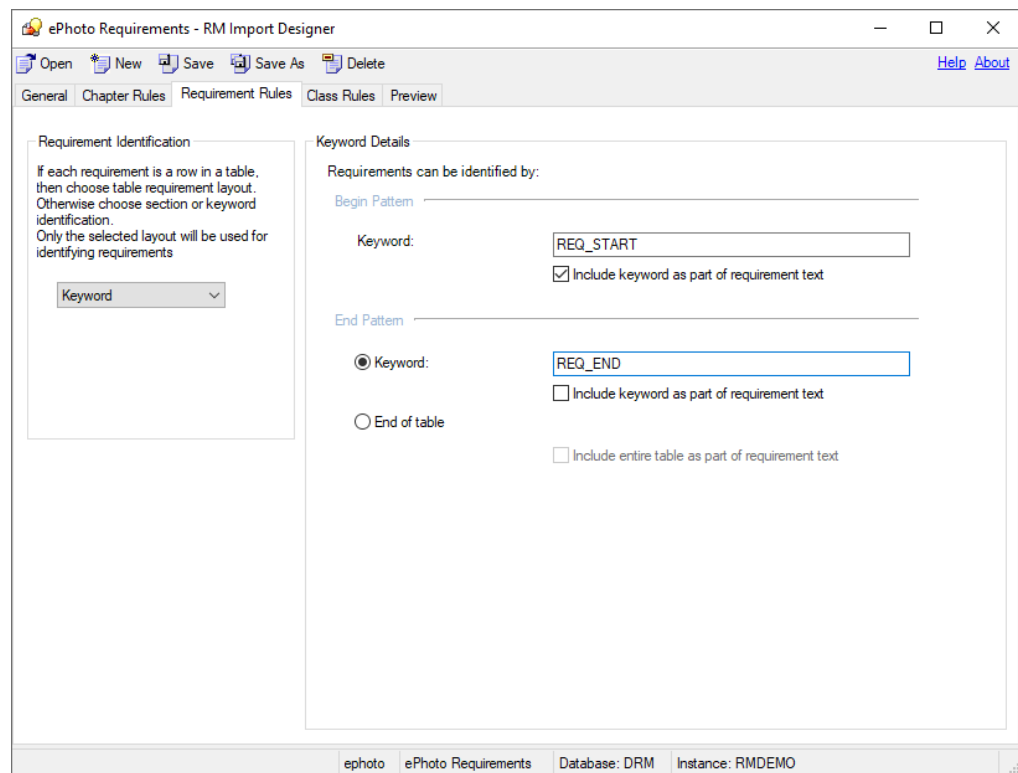
**To complete the Requirement Rules tab for the Section option:**

- 1 Under **Requirement Identification**, select **Section**.
- 2 Under **Section Details**, select one of the options described in the following table.

Option	Description
All paragraphs	Select this option to identify every paragraph in a chapter as a requirement. This option is useful for numbered lists, bulleted lists, and so on.
All paragraphs containing keyword	<p>Select this option to identify every paragraph in the chapter as a requirement only if it contains the keyword or keywords you type in the field. <i>Shall</i>, <i>will</i>, and <i>must</i> are examples of keywords you could type here. You can also type regular Word expressions in this field. For examples of regular Word expressions, see <a href="#">"Word Regular Expressions" on page 425</a>.</p> <p><b>NOTE:</b> When there is information between two paragraphs that contain keywords, that information is captured into the first requirement.</p> <p>To perform an OR search, separate multiple keywords with spaces. If you want to search for an exact string, enclose multiple keywords in quotation marks.</p> <p>To perform a customized search, use a regular expression.</p>
Only paragraphs with these heading styles...	<p>Select this option to identify any block of text with a specific heading style as a requirement. The heading is included as part of the requirement.</p> <p>If you want to include custom headings, click <b>Load custom headings</b> and type or browse to the Word document from which you want to load custom styles. Select those headings that you want to use to identify requirements.</p> <p><b>NOTE:</b> If you imported custom headings on the <b>Chapter Rules</b> tab, this list is automatically populated with the headings from the document you specified there.</p>

**Keyword Option**

If requirements cannot be identified using the table or section rules, you can specify a pattern using a keyword or Word regular expression that identifies requirements. The pattern can span paragraphs and the first match of the "begin pattern" keyword represents the beginning of the requirement. You can identify an entire table representing a requirement using this option.



**Figure 13-8. Requirement Tab—Keyword Option**

**To complete the Requirement Rules tab for the Keyword option:**

- 1 Under **Requirement Identification**, select **Keyword**.



#### NOTES

- Keywords are case sensitive. To search for either case, type both words in the **Keyword** box, separated by a space. For example, type **design Design**.
- To perform a customized search, use a regular expression. For information about regular expressions, see "[Word Regular Expressions](#)" on page 425.

- 2 Under **Begin Pattern**, type the keyword or keywords or Word regular expression that marks the beginning of the requirement. If you want to include the keyword as part of the requirement, select the **Include keyword as part of requirement text** check box.

This field is mandatory.

- 3 Under **End Pattern**, do one of the following:
  - Select **Keyword** and type the keyword or keywords or Word regular expression that marks the end of the requirement. If you want to include the keyword as part of the requirement, select the **Include keyword as part of requirement text** check box.
  - Select **End of table** if the beginning keyword is before the table and the entire table after the beginning keyword represents a requirement. If you want to include the entire table as part of the requirement, select the **Include entire table as part of requirement text** check box.

## Class Rules Tab

The **Class Rules** tab allows you to identify classes in a document and set up default attributes and categories. By default, the title and description attributes and other attributes that are specified as "mandatory" in Class Definition are included in each class.

RM Import attempts to capture everything that is not a requirement as the chapter description. It attempts to capture portions of a requirement that are not captured into any attribute into the default Description attribute of that class.



**CAUTION!** If you do not enable HTML formatting for the default Description attribute or any other text attribute, then formatting and images are not imported. For instructions for enabling HTML for text attributes, see ["Text Attribute" on page 291](#).



**CAUTION!** If you delete a class that is referenced in a template from Class Definition, or remove "read" permission for it, the template becomes invalid.



**NOTE** If the entire requirement can be captured into the default Description attribute, then you do not have to make any additional choices on the **Class Rules** tab.

### Class Information



**NOTE** A red exclamation mark indicates that a mandatory default value must be specified.

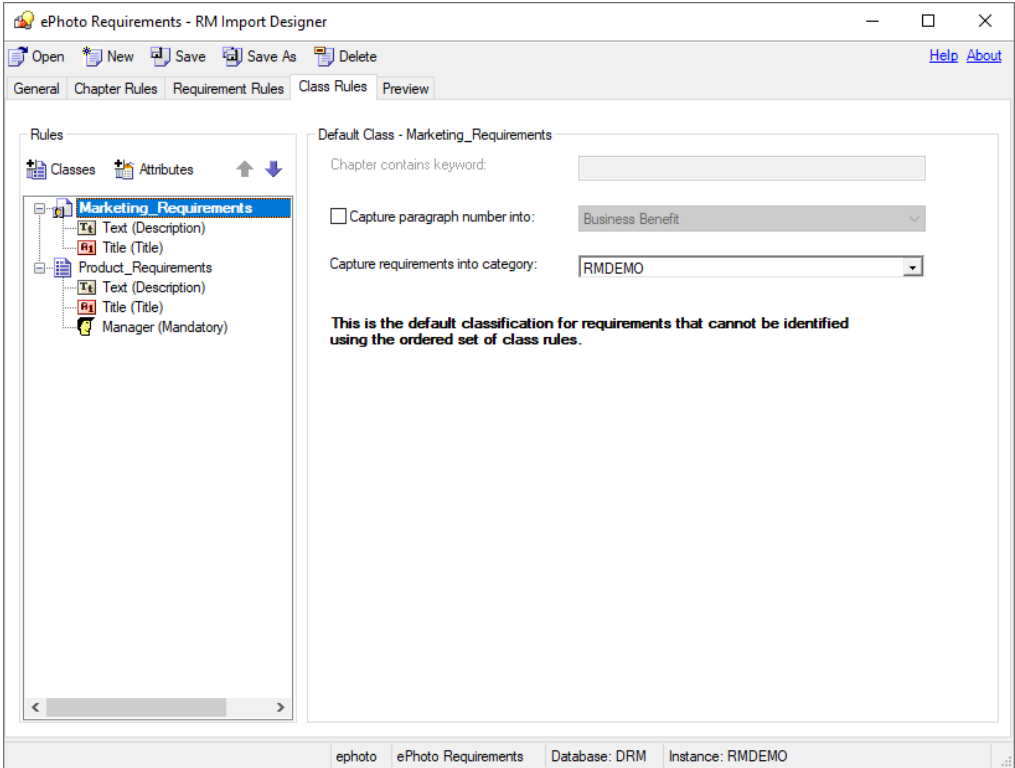


Figure 13-9. Class Rules Tab—Default Class

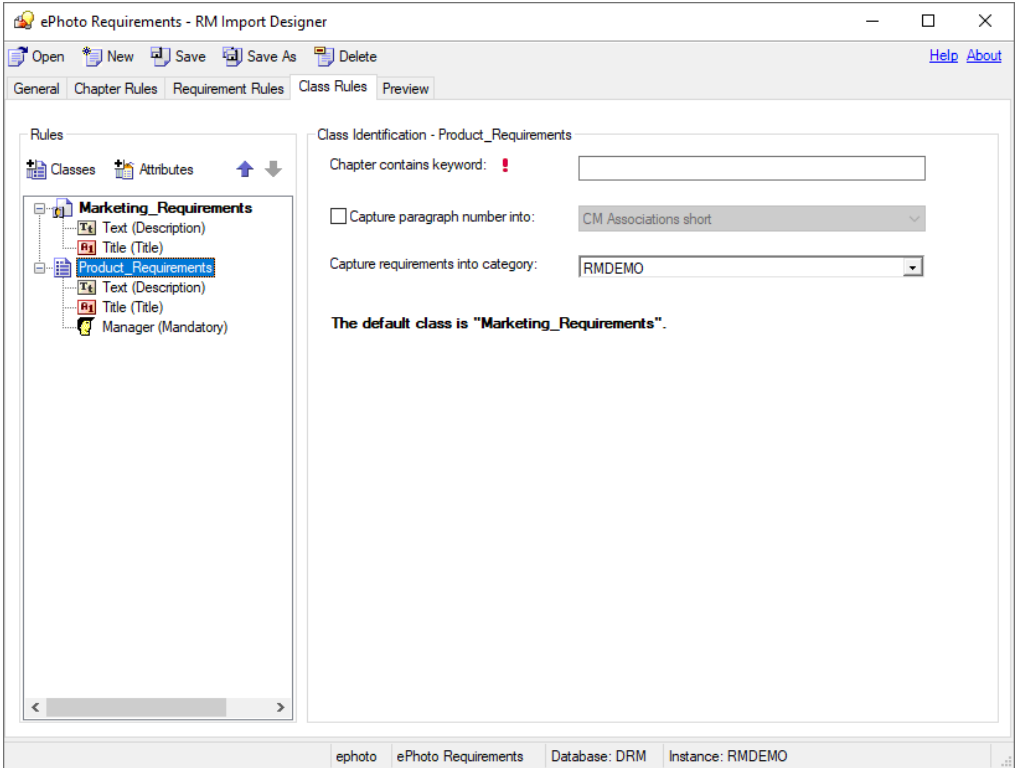
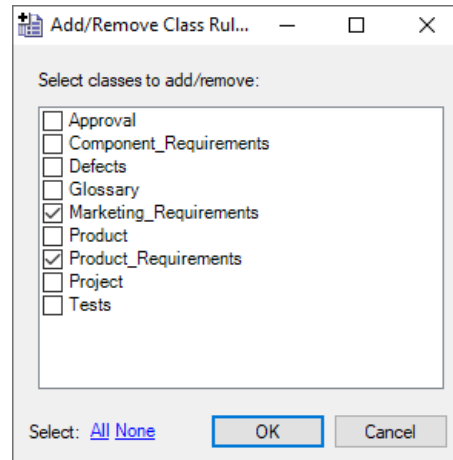


Figure 13-10. Class Rules Tab—Non-Default Class

**To complete the Class Rules tab for a class:**

- 1 Do one of the following:
  - If you are creating a new template, the **Add/Remove Class Rules** dialog box automatically opens when you click the **Class Rules** tab. Proceed to the next step.
  - If you need to change the classes that are included in an existing template, click **Classes**, or right-click in the left pane and select **Add/Remove Classes**.

The **Add/Remove Class Rules** dialog box opens.



**Figure 13-11. Add/Remove Class Rules**

- 2 A set of class types that are defined for the instance are listed. Select the classes into which you want to import requirements and click **OK**. To select all of the classes, click **All** at the bottom of the dialog box and click **OK**.
- 3 By default, the first class listed in the **Add/Remove Class Rules** dialog box becomes the default class for all requirements, and is displayed in boldface type. To change the default class, select the class you want as the default class, right-click in the left pane, and click **Mark as default**.



**NOTE** You can define only one default class for each template.

- 4 To remove a class, click the **Classes** button, or right-click in the left pane and select **Add/Remove Classes**. In the **Add/Remove Class Rules** dialog box that opens, clear the check box for the class and click **OK**.

Alternatively, you can right-click the class in the left pane and click **Remove**.

- 5 Each chapter that contains requirements is searched for keywords. In the **Chapter contains keyword** box, type the keyword or Word regular expression that identifies the class. If there is a match, then requirements found in the chapter are imported as requirements of that class.

This is important when multiple classes can be identified from the document. The keywords are searched in the order in which the classes are specified in the **Add/**

**Remove Class Rules** dialog. To reorder the classes, select the class and then click the up or down arrow in the left pane.



#### NOTES

- The **Chapter contains keyword** field is disabled for the default class, because all requirements found in the document are of the same class.
- To perform a customized search, use a regular expression. For information about regular expressions, see ["Word Regular Expressions" on page 425](#).

- 6 If you want to import the paragraph ID (for example, 5.3.2) into an attribute, select the **Capture Paragraph Number into** check box and select the attribute from the list.
- 7 Select the category to which the requirement will belong from the **Capture requirements into category** list. The default is the root category (the instance). The category that you select respects the category permissions for the user.

## Attribute Information

When a class in the left pane is expanded, you can select an attribute and specify how the attributes within a requirement are identified, specify default values, and so on. The information in the right pane varies depending on the **Requirement Identification** option selected on the **Requirement Rules** tab, and the type of attribute that is selected. The option that was selected on the **Requirements Rules** tab is displayed at the top of the **Class Rules** tab when an attribute is selected in the left pane.



**CAUTION!** If you delete an attribute that is referenced in a template from Class Definition, the template becomes invalid.



#### NOTES

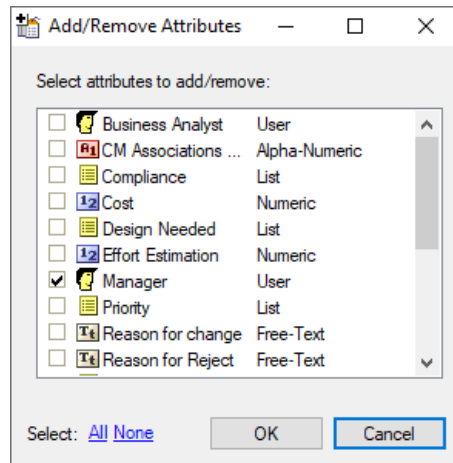
- The same region within a requirement can be captured into multiple attributes. For example, the third column in a table can be captured into more than one attribute.
- A red exclamation mark indicates that a mandatory default value must be specified. The title and description attributes always require default values, as well as attributes that are marked as mandatory in Class Definition.

### ***Adding and Removing Attributes***

**To add and remove attributes from a class:**

- 1 Select the class to which you want to add attributes.
- 2 Click **Attributes**, or right-click in the left pane and click **Add/Remove Attributes**.

The **Add/Remove Attributes** dialog box opens. All of the attributes that are defined for the class are listed.



**Figure 13-12. Add/Remove Attributes**

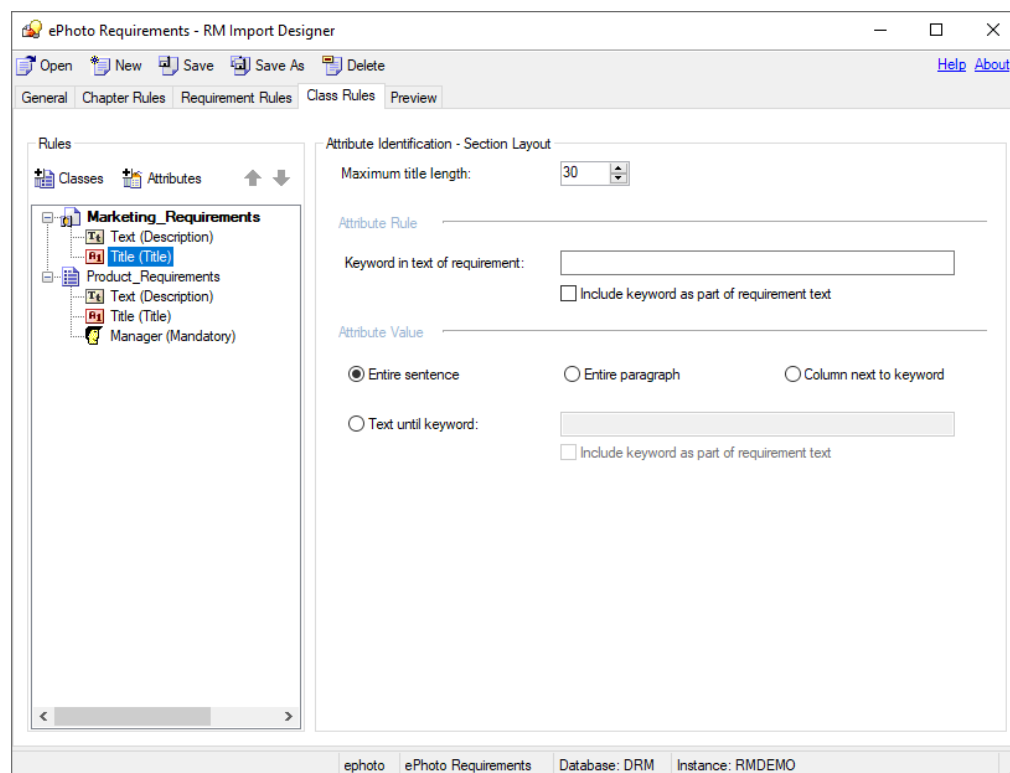
- 3 Select the attributes that you want to add and click **OK**. To select all attributes, click **All** at the bottom of the dialog box and click **OK**.
- 4 To remove an attribute, click **Attributes**, or right-click the attribute in the left pane and click **Add/Remove Attributes**. In the **Add/Remove Attributes** dialog box that opens, clear the attribute check box and click **OK**. To remove all attributes, click **None** at the bottom of the dialog box and click **OK**.



**NOTE** Default and mandatory attributes for the selected class are always selected and cannot be removed.

## Alphanumeric Attributes with Section or Keyword Option

The following illustration shows the **Class Rules** tab for alphanumeric attributes with the Section or Keyword option:



**Figure 13-13. Class Rules Tab—Section or Keyword Option—Alphanumeric Attributes**

**To complete the Class Rules tab for alphanumeric attributes with the Section or Keyword option:**

- 1 In the **Maximum title length** field, select the number of characters for the attribute title. The default value is **30**.
- 2 In the **Keyword in text of requirement** field, type the keyword, keywords, or Word regular expression to identify the attribute. If you want to include the keyword as part of the requirement, select the **Include keyword as part of requirement text** check box. If no rule is specified in this field, by default the first 30 characters are captured as the title.



**NOTE** To perform a customized search, use a regular expression. For information about regular expressions, see ["Word Regular Expressions" on page 425](#).

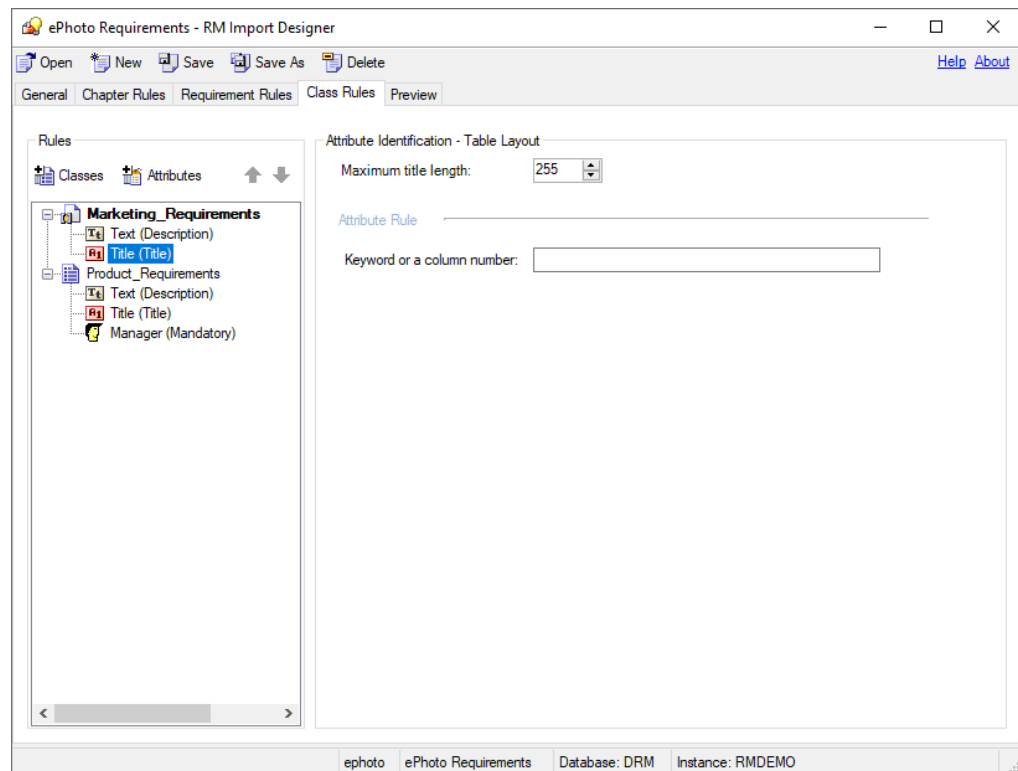
- 3 Under **Attribute Value**, specify one of the options described in the following table:

Option	Description
Entire sentence	The entire sentence in which the keyword is found is the attribute value.
Entire paragraph	The entire paragraph in which the keyword is found is the attribute value.

Option	Description
Column next to keyword	The requirement includes a table, and the entire content of the cell to the right of the first cell containing the keyword is the attribute value. When the cell that contains the keyword is the last cell in a row, the content of the first cell in the next row is the attribute value. <b>NOTE:</b> This does not pertain to the Table option.
Text until keyword	The text up to the specified keyword is the attribute value. Select the <b>Include keyword as part of requirement</b> check box if you want to include the keyword in the attribute value. The default is to exclude the keyword.

### Alphanumeric Attributes with Table Option

The following illustration shows the Class Rules tab for alphanumeric attributes with the Table option:



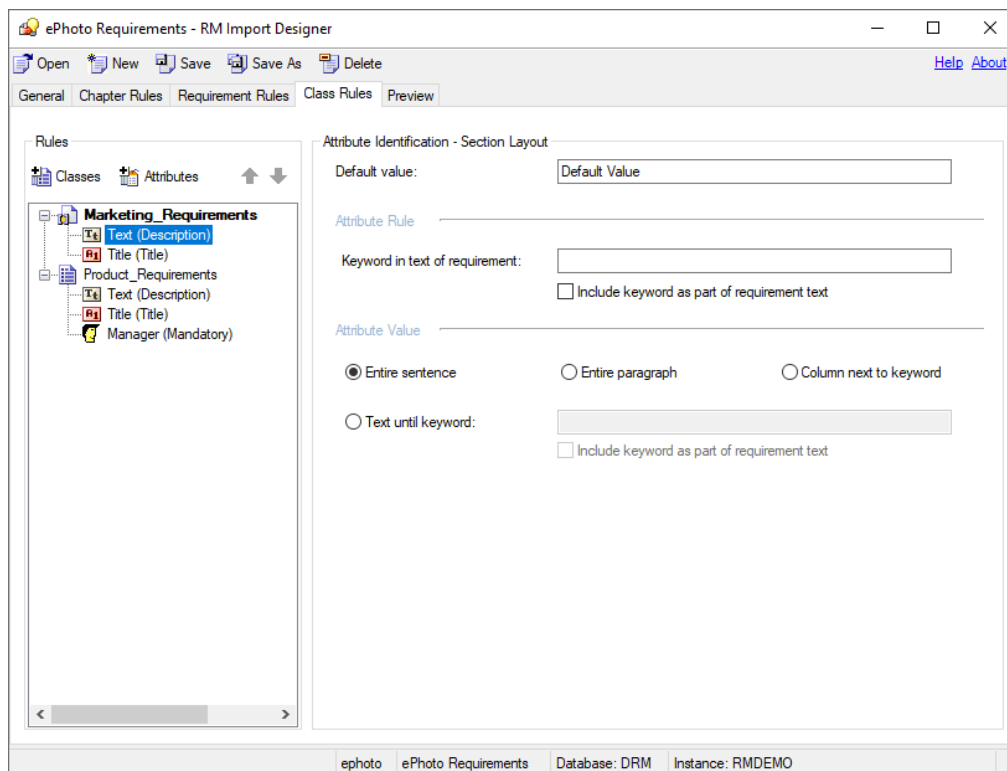
**Figure 13-14. Class Rules Tab—Table Option—Alphanumeric Attributes**

**To complete the Class Rules tab for alphanumeric attributes with the Table option:**

- 1 In the **Maximum title length** field, select the number of characters for the attribute title. The default value is **30**.
- 2 In the **Keyword or column number field**, type the keyword or column number to identify the attribute. For example, if the **Priority** attribute is in the third column, you could specify 3. The information specified in the cell below the column heading represents the value of the attribute (for example, **H i g h**). If no rule is specified in this field, by default the first 30 characters are captured as the title.

## Text or Numeric Attributes with Section or Keyword Option

The following illustration shows the **Class Rules** tab for text or numeric attributes with the Section or Keyword option:



**Figure 13-15. Class Rules Tab—Section or Keyword Option—Text or Numeric Attributes**

**To complete the Class Rules tab for text or numeric attributes with the Section or Keyword option:**

- 1 In the **Default value** field, type a default value for the attribute value if the attribute value cannot be found in the document. For numeric attributes, you must enter a number. This field must be filled in for mandatory attributes.

For example, for the **Owner** attribute, you could set the default value to the name of the team lead for the instance.

- 2 In the **Keyword in text of requirement** field, type the keyword, keywords, or Word regular expression to identify the attribute. If you want to include the keyword as part of the requirement, select the **Include keyword** check box.



**NOTE** To perform a customized search, use a regular expression. For information about regular expressions, see "[Word Regular Expressions](#)" on page 425.

- 3 Under **Attribute Value**, specify one of the options described in the following table:

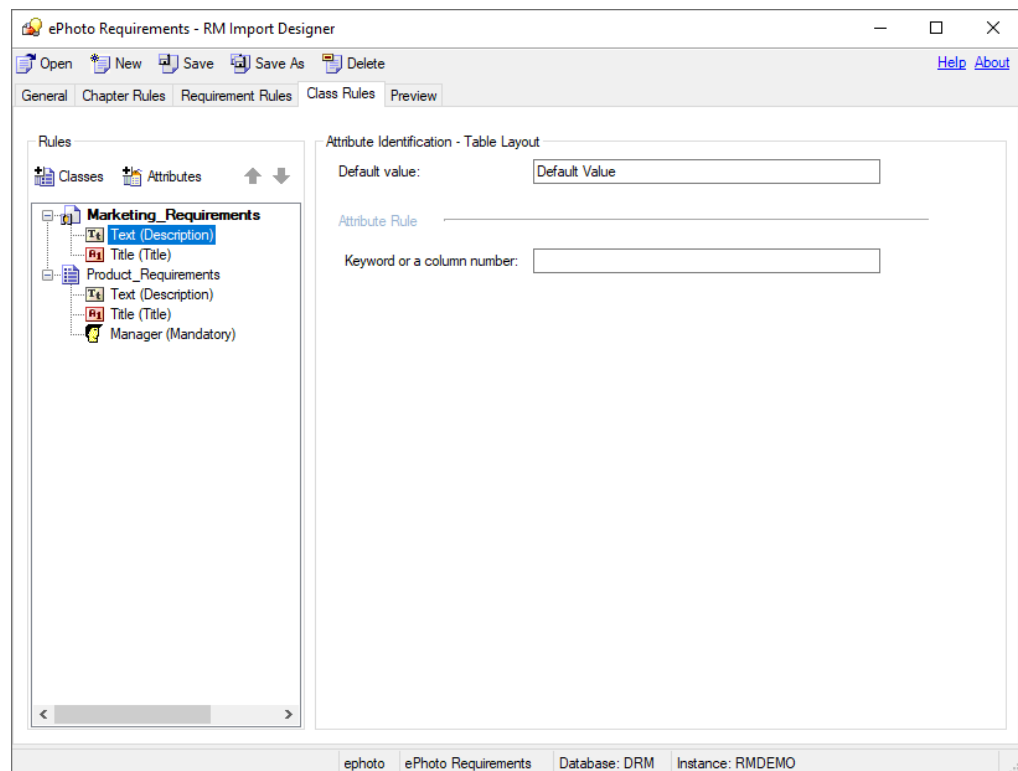
Option	Description
Entire sentence	The entire sentence in which the keyword is found is the attribute value.
Entire paragraph	The entire paragraph in which the keyword is found is the attribute value.
Column next to keyword	The requirement includes a table, and the entire content of the cell to the right of the first cell containing the keyword is the attribute value. When the cell that contains the keyword is the last cell in a row, the content of the first cell in the next row is the attribute value. <b>NOTE:</b> This does not pertain to the Table option.
Text until keyword	The text up to the specified keyword is the attribute value. Select the <b>Include keyword</b> check box if you want to include the keyword in the attribute value. The default is to exclude the keyword.



**NOTE** If you do not choose an **Attribute Value** option, the attribute value is the text following the keyword until the next keyword is found or the end of the chapter or document is reached.

### **Text or Numeric Attributes with Table Option**

The following illustration shows the **Class Rules** tab for text or numeric attributes with the Table option:



**Figure 13-16. Class Rules Tab—Table Layout—Text or Numeric Attributes**

### To complete the Class Rules tab for text or numeric attributes with the Table option:

- 1 In the **Default value** field, type a default value for the attribute value if the attribute value cannot be found in the document. For numeric attributes, you must enter a number. This field must be filled in for mandatory attributes.

For example, for the **Priority** attribute, you could set the default value to Low.



**NOTE** A red exclamation mark indicates that a mandatory default value must be specified. The title and description attributes always require default values, as well as attributes that are marked as mandatory in Class Definition.

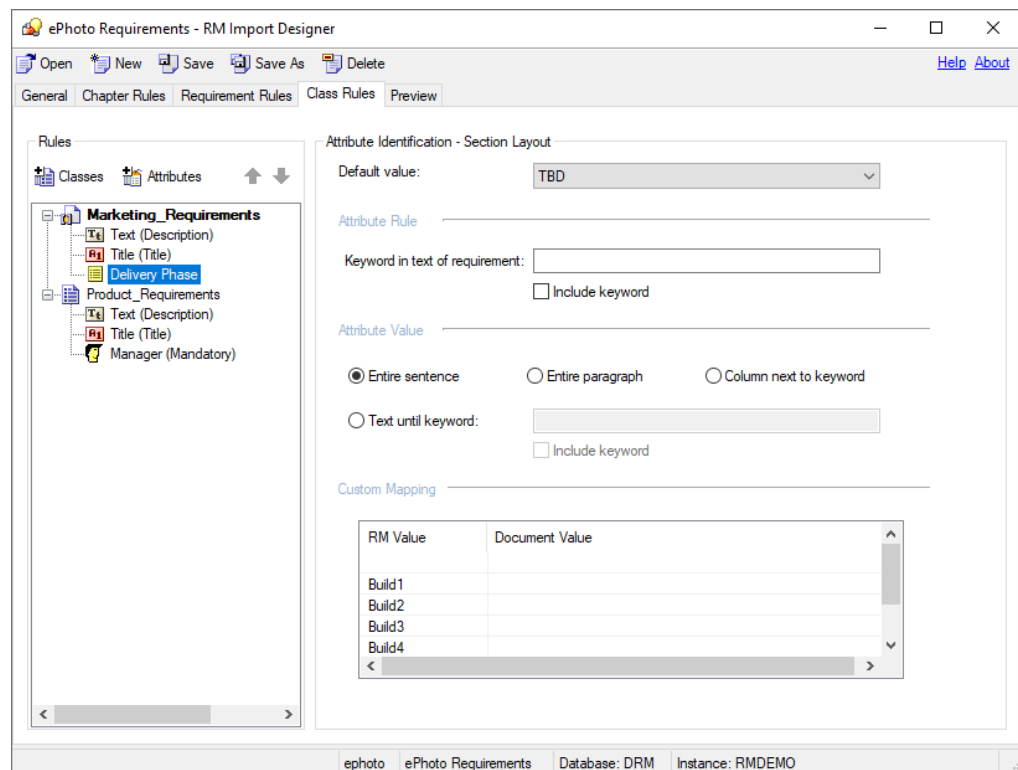
- 2 In the **Keyword or a column number** field, type the keyword or column number to identify the attribute. For example, if the **Priority** attribute is in the third column, you could specify 3. The information specified in the cell below the column heading represents the value of the attribute (for example, High).



**NOTE** To perform a customized search, use a regular expression. For information about regular expressions, see "[Word Regular Expressions](#)" on page 425.

### List or User Attributes with Section or Keyword Option

The following illustration shows the **Class Rules** tab for list or user attributes with the Section or Keyword option:



**Figure 13-17. Class Tab—Section or Keyword Layout—List or User Attributes**

**To complete the Class tab for list or user attributes with a Section or Keyword layout:**

- 1 In the **Default Value** field, select the default value for the attribute if the attribute value cannot be found in the document. For example, for a **Delivery Phase** attribute, you could select TBD (To Be Determined).
- 2 In the **Keyword in text of requirement** field, type the keyword, keywords, or Word regular expression to identify the attribute. If you want to include the keyword as part of the requirement, select the **Include keyword** check box. The **Keyword in text of requirement** field must be filled in for mandatory attributes.



**NOTES**

- A red exclamation mark indicates that a mandatory keyword must be specified.
- To perform a customized search, use a regular expression. For information about regular expressions, see ["Word Regular Expressions" on page 425](#).

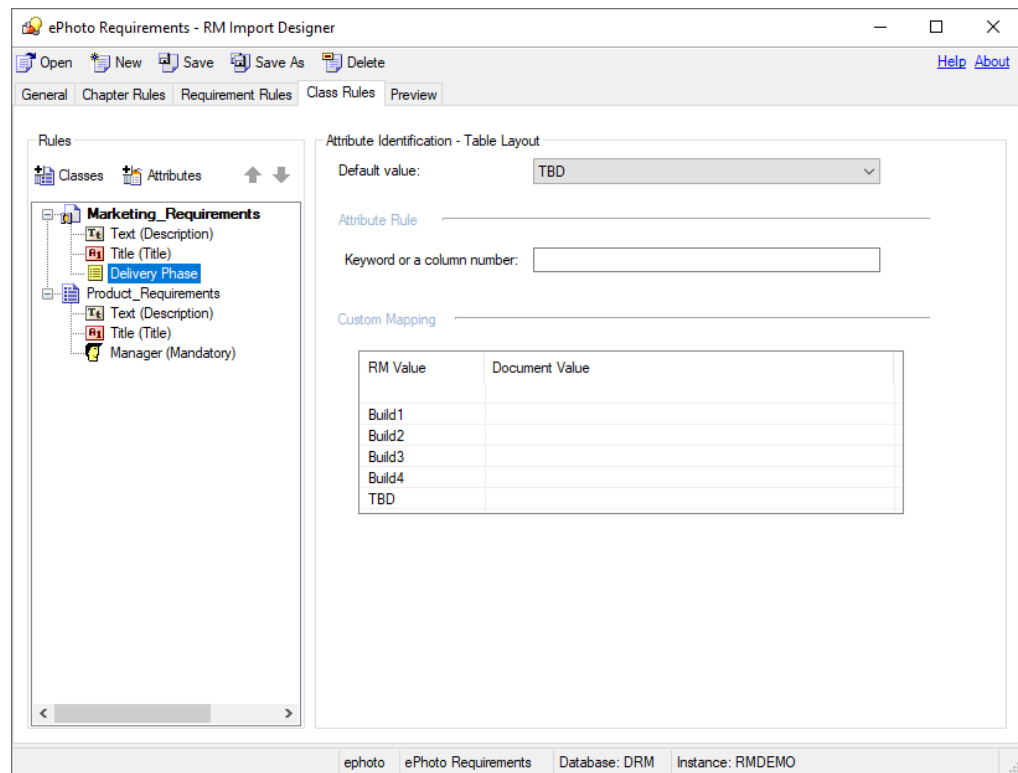
- 3 Under **Attribute Value**, specify one of the options described in the following table:

Option	Description
Entire sentence	The entire sentence in which the keyword is found is the attribute value.
Entire paragraph	The entire paragraph in which the keyword is found is the attribute value.
Column next to keyword	The requirement includes a table, and the entire content of the cell to the right of the first cell containing the keyword is the attribute value. When the cell that contains the keyword is the last cell in a row, the content of the first cell in the next row is the attribute value. <b>NOTE:</b> This does not pertain to the Table option.
Text until keyword	The text up to the specified keyword is the attribute value. Select the <b>Include keyword</b> check box if you want to include the keyword in the attribute value. The default is to exclude the keyword.

- 4 If you want to map values from the document to the actual values in the Dimensions RM database, under **Custom Mapping**, enter the values under **Document Value**. Separate multiple values with commas. If you map values, the Dimensions RM values appear in the imported document instead of the document values. For example, Build 3 is the value in the Dimensions RM database, but Alpha is the corresponding value in the document.

## List or User Attributes with Table Option

The following illustration shows the **Class Rules** tab for list or user attributes with the Table option:



**Figure 13-18. Class Rules Tab—Table Layout—List or User Attributes**

**To complete the Class Rules tab for list or user attributes with the Table option:**

- 1 In the **Default value** field, select the default value for the attribute if the attribute value cannot be found in the document. For example, for a **Verification Status** attribute, you could select **Not Scheduled**.
- 2 In the **Keyword or a column number** field, type the keyword or column number to identify the attribute. For example, if the **Verification Status** attribute is in the third column, you could specify 3. The information specified in the cell below the column heading represents the value of the attribute (for example, **Passed**).



**NOTE** To perform a customized search, use a regular expression. For information about regular expressions, see ["Word Regular Expressions" on page 425](#).

- 3 If you want to map values from the document to the actual values in the Dimensions RM database, under **Custom Mapping**, enter the values under **Document Value**. Separate multiple values with commas. If you map values, the Dimensions RM values appear in the imported document instead of the document values. For example, **Scheduled** is the value in the Dimensions RM database, but **Committed** is the corresponding value in the document.

## Preview Tab

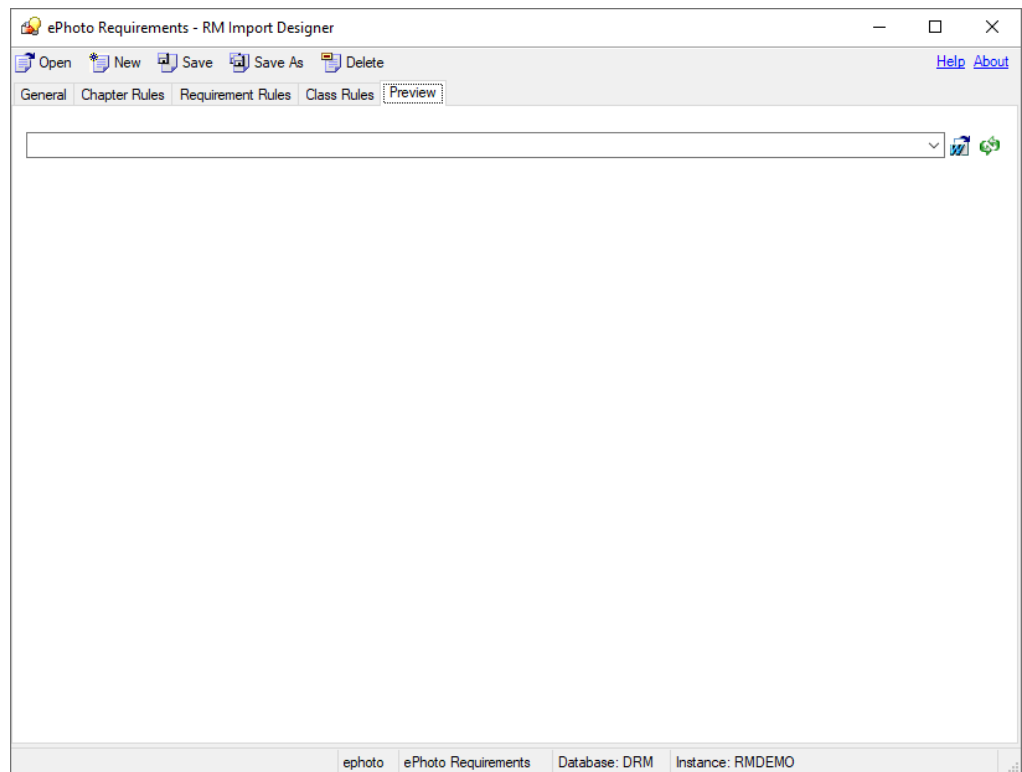
The **Preview** tab allows you to see approximately how the document would look in Documents View if it were imported using the template you are working with. The preview appears in a tree-like structure in the left pane.





**NOTE** If the Word document is set to "Protected" mode with a read-only restriction, an error message could be displayed in the preview screen. To prevent this problem, copy all of the information from the protected Word document and paste it into a new Word document.

### To preview the document:

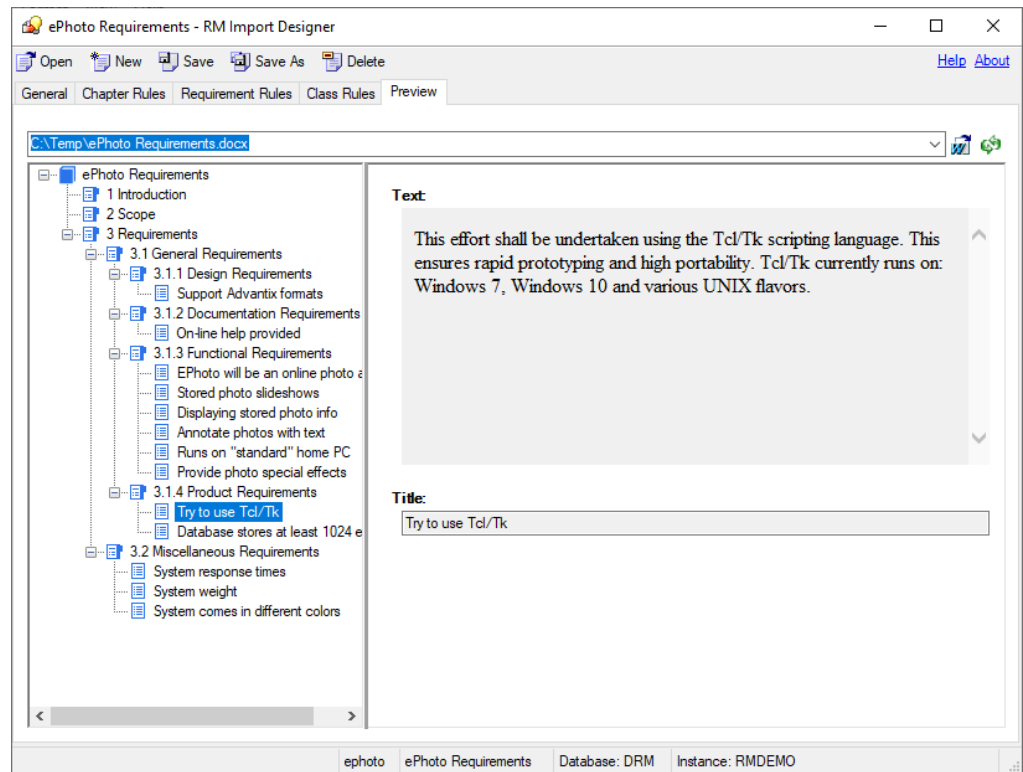
- 1 Click the **Preview** tab.



**Figure 13-19. Empty Preview Tab**

- 2 Do one of the following:
  - Click the **Select a document to load** button . The **Open** dialog box opens. Select the document you want to preview and click **Open**.
  - Click the **Load the currently selected document** button . Use this option if you made changes to the Word document and want to rerun the parser, or if you selected a previously viewed document in the dropdown list.

The **Parsing Word Document** dialog box shows you the progress of the document parsing. Click **Close** when the parsing is complete. The document structure is displayed in the left pane.



**Figure 13-20. Preview Tab**

## Word Regular Expressions

A number of fields can contain keywords or regular expressions. The content of these fields can either be text that is to be matched (such as "shall") or a Word regular expression.



**TIP** Before you type a regular expression in a field in RM Import Designer, test it in Word on the document you are going to parse. To do so, open the Word document, Select **Edit | Find**, click **More**, select **Use Wildcards**, and then type the expression in the **Find What** field. You can also click **Special** to select wildcard characters that can be used to build regular expressions.

This section briefly describes how to use Word regular expressions, and provides some examples of their use.



**NOTE** For comprehensive information about using Word regular expressions, refer to Microsoft documentation.

Word provides a set of wildcard characters that you can use to build regular expressions.

- A **wildcard character** is a keyboard character that represents one or many characters.
- A **regular expression** is a combination of literal and wildcard characters that you use to find text patterns. For example, if you want to search for "manage" but not "management," type **<manage>** instead of **manage**.

The following table lists the wildcard characters that you can use in Word.

Text to Search	Wildcard Character	Examples
Single character	?	<b>a?t</b> finds "act" and "art." It also finds these characters within a word (for example, "action" and "artist").
String of characters	*	<b>p*d</b> finds "pad" and "passed." The asterisk returns all characters and spaces that are between the specified literal characters.
Beginning of word	<	<b>&lt;(para)</b> finds all words that start with "para," such as "parakeet" and "paragraph."
End of word	>	<b>(out)&gt;</b> finds all words that end with "out," such as "about" and "without" but not "outstanding."
One or more specified characters	[ ]	<b>s[io]n</b> finds "sin" and "son," but not "skin," because "k" is not specified within the brackets.
Single character in a range of characters	[x-z]	<b>[b-s]ought</b> finds "bought," "fought," and "sought." The range must be in ascending order (for example, b-s is correct, but not s-b)
Single character except the characters in the range inside the brackets	[!x-z]	<b>h[!a-m]ck</b> finds "hock," but not "hack" or "hick."
Exactly <i>n</i> occurrences of the previous character or expression	{ <i>n</i> }	<b>me{2}t</b> finds "meet" but not "met." <b>h[a-z]{2}d</b> finds "heed," "hand," and "hind," but does not find "hid" or "had". <b>h([a-z]){2}d</b> finds "heed" but not "hand" or "hind."
At least <i>n</i> occurrences of the previous character or expression	{ <i>n</i> ,}	<b>lo{1,}t</b> finds "loot" and "lot."
From <i>n</i> to <i>m</i> occurrences of the previous character or expression	{ <i>n</i> , <i>m</i> }	<b>30{1,3}</b> finds "30," "300," and "3000."
One or more occurrences of the previous character or expression	@	<b>ro@t</b> finds "rot" and "root."

Text to Search	Wildcard Character	Examples
Any wildcard character	<code>\wildcard_character</code>	<code>[\?]</code> finds all question mark wildcards, <code>[\*]</code> finds all asterisk wildcards, and so on.
To group characters and set orders of evaluation	<code>()</code>	<code>h([a-z]){2}d</code> finds "heed" but not "hand," "hind" or "had."



**NOTE** Wildcard searches are case sensitive.

## Example Word Regular Expressions

The following table contains example Word regular expressions that you could use in your templates.

Word Regular Expression	Description
<code>RQMT_[0-9]@</code>	Finds sequences that start with "RQMT_" and any number of numbers. For example, <b>RQMT_0009</b> .
<code>\&lt;\&lt;SYS[0-9]@\&gt;\&gt;</code>	Finds sequences that start with <<, then "SYS" and any number of numbers, and that end with >>. For example, <b>&lt;&lt;SYS0109&gt;&gt;</b> .
<code>[0-9].</code>	Finds sequences that start with any number and a period. For example, <b>24.</b>
<code>0[0-9]@</code>	Finds sequences that start with 0 followed by any number of numbers. For example, <b>0008</b> .
<code>[0-9].[0-9].[0-9]</code>	Finds sequences that start with three numbers separated by decimal points. For example, <b>1.2.6</b> .

## Limitations

This section describes some limitations of the RM Import tool. Be sure to take these limitations into consideration when you design templates.



**IMPORTANT!** Before you prepare a template that will be used to import a Word document, save the document as HTML and examine the results. This is the way the document will be displayed in RM Browser after it is imported. If you see any formatting problems that are unacceptable (for example, problems with lists, bullets, and fonts), adjust the styles used in the Word document until the results are satisfactory.

- Microsoft Word uses unique, proprietary styles and formatting; therefore, the styles and formatting of the Word document (for example, lists, bullets, and fonts) are not necessarily preserved in Document View. However, the text is always imported, so there is no data loss.
- You cannot import the changes you make in Document View back into the original Word document. Roundtripping between Dimensions RM and Word is not supported.

- Custom headings that you create based on standard Word headings are imported as standard Word headings, not as custom headings.
- On the **Requirement Rules** tab for the Keyword option:
  - If you select the **Include entire table as part of requirement text** check box, the keyword must be in the table to be included as part of the requirement. The entire table that contains the keyword is the requirement.
  - If you do *not* select the **Include entire table as part of requirement text** check box, and if the **Begin Pattern** keyword is found and the end of the chapter is reached, the table is included as part of the requirement.
  - If the keyword you typed under **Begin Pattern** is found and the end of the chapter is reached, the requirement is captured, even if the keyword you typed under **End Pattern** is not at the end of the chapter.
- Importing every cell in a table as a requirement is not supported.
- If a list number in the Word document is preceded by text (such as *Requirement#*), the text is not imported. Therefore, *Requirement #1* in the Word document is imported as *1*.
- If you use the **Entire sentence** option to capture attributes, lists in the Word document might not be imported.

## Examples

["RM Import Designer Examples" on page 471](#) contains examples of Word documents and explains how their structure determines how you set up templates for them.

# Appendix A

---

## Handling Certificates

Importing a PFX Certificate into Microsoft IIS	430
Importing a PFX Certificate into Windows	430
Exporting Certificates	432
Listing all Certificates in a Keystore	439
Retrieving the Alias from a PFX File	439
Retrieving Root CA and Intermediate CA Certificate Files	440
Importing Root and Intermediate CA into Local Certificate Store	442

## 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 raises 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 430](#). 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 434).

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 434](#)).

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 432).

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

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

- 1 On the server, open a command prompt.
- 2 Enter mmc and press **Enter** to start the Microsoft Management Console.
- 3 From the **File** menu, select **Add/Remove Snap-in...** or press **Ctrl+M**.
- 4 From the list **Available snap-ins**, select **Certificates**.
- 5 Click **Add**.

- 6 In the **Certificates snap-in** dialog, do the following:
  - a Select **Computer account**.
  - b Click **Next**.
  - c Ensure that option **Local computer: (the computer this console is running on)** is selected.
  - d Click **Finish**.
- 7 Click **OK**.
- 8 Expand **Certificates (Local Computer)**.
- 9 Locate the certificate in the tree. Common locations are:
  - Personal | Certificates
  - Trusted Root Certification Authorities | Certificates
- 10 Right-click the certificate and select **All Tasks | Export** from the shortcut menu. This opens the **Certificate Export Wizard**.
- 11 Click **Next**.
- 12 Select the option **Yes, export the private key**.
- 13 Click **Next**.
- 14 Ensure that option **Personal Information Exchange - PKCS #12 (.PFX)** is selected.
- 15 Select the following options:
  - **Include all certificates in the certification path if possible**
  - **Export all extended properties**
- 16 Click **Next**.
- 17 Enter a password into the **Password** and **Type and confirm password (mandatory)** boxes. Take a note of that password.
- 18 Click **Next**.
- 19 Click **Browse...** to open a dialog to save the certificate.
- 20 Select the target directory and specify a file name.
- 21 Click **Save**.
- 22 Click **Next**.
- 23 Click **Finish** and confirm the success message.

## Exporting Certificates to PFX Format from IIS

A certificate in PFX format is required for import into the ssl keystore (e.g. sample-ssl.jks) in Tomcat's conf directory. For all other keystores, use the CER format (see chapter ["Exporting Certificates to CER Format from the Management Console"](#) on page 432).

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

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

- 1** Do one of the following:
  - Start the **Server Manager**, and expand **Roles** followed by **Web Server (IIS)**.
  - Start the **Computer Management Console** by running the command `compmgmt.msc`, and expand **Services and Applications**.
  - Right-click on the Computer icon, select **Manage** from the resulting menu, and expand **Services and Applications**.
- 2** Select **Internet Information Server (IIS) Manager**.
- 3** In the **Connections** pane, select a computer node.
- 4** On the **Home** pane, double-click the **Server Certificates** icon.
- 5** Double-click the IIS certificate. This opens the **Certificate** dialog.
- 6** Select the **Details** tab.
- 7** Click **Copy to File**. This opens the **Certificate Export Wizard**.
- 8** Click **Next**.
- 9** Select the option **Yes, export the private key**.
- 10** Click **Next**.
- 11** Ensure that option **Personal Information Exchange - PKCS #12 (.PFX)** is selected.
- 12** Select the following options:
  - **Include all certificates in the certification path if possible**
  - **Export all extended properties**
- 13** Click **Next**.
- 14** Enter a password into the **Password** and **Type and confirm password (mandatory)** boxes. Take a note of that password.
- 15** Click **Next**.
- 16** Click **Browse...** to open a dialog to save the certificate.
- 17** Select the target directory and specify a file name.
- 18** Click **Save**.
- 19** Click **Next**.
- 20** Click **Finish** and confirm the success message.



**NOTE** Do not use a self-signed certificate on the RM Web Server.

## Exporting a Certificate from the STS Server from the Command Prompt

When using SBM, you can export the STS certificate through SBM configurator (see chapter "Exporting the STS Certificate from SBM Configurator" on page 438).

### 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\Open Text\Dimensions 12.12`.
- Replace *###.#* with the Common Tools version number, e.g. `2.3.0.0`.
- Replace *##* with the Java version number, e.g. `11.0`.

The complete set command may look like this:

```
set path=%path%;"C:\Program Files\Open Text\Dimensions
12.12\Common Tools 2.3.0.0\jre\11.0.bin"
```

- 3 Type the following command (all on one line) and press **Enter**:  
`keytool -export  
-keystore keystore.jks -storepass StorePassword  
-alias sts -file CerPath`



#### NOTE

- Replace *StorePassword* with the password for the keystore. The default for `keystore.jks` is **changeit**
- Replace *CerPath* with the full path to your certificate in CER format. If the path contains spaces, surround the path with double quotes.

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

```
keytool -export -keystore keystore.jks -storepass MyPassword  
-alias sts -file "C:\My Certificates\MyCert.cer"
```

- 4 To convert the certificate to PEM format, type the following openssl command and press **Enter**:  
`openssl x509 -in CerPath -inform DER -out PemPath -outform PEM`



#### NOTE

- You can obtain an openssl binary from <http://www.openssl.org/>.
- Replace *CerPath* with the full path to your certificate in CER format. If the path contains spaces, surround the path with double quotes.
- Replace *PemPath* with the full path you want to save the certificate in PEM format to. If the path contains spaces, surround the path with double quotes.

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

```
openssl x509 -in "C:\My Certificates\MyCert.cer" -inform DER  
-out "C:\My Certificates\MyCert.pem" -outform PEM
```

## Exporting the STS Certificate from SBM Configurator

When using SBM, you can export the STS certificate through SBM configurator, which allows exporting the certificate into various formats.

**To export the STS certificate, do the following:**

- 1 Start **SBM Configurator**.
- 2 In the **Advanced** set, select **Security**.
- 3 In the **Components** list, ensure that **STS** is selected.
- 4 Click **Actions**. This opens a shortcut menu.
- 5 From the shortcut menu, select **Export Certificate**. This opens the **Save As** dialog.
- 6 In the **Save as type** box, select the desired format.



#### NOTE

- If you require the certificate for copying it to *RM\_Install\RM\conf*, choose **(\* .pem)**.
- If you require the certificate for importing it into a keystore (e.g. truststore.jks), choose **(\* .cer)**.

- 7 Navigate to a directory to which you want to save the file to.
- 8 Enter a file name (e.g. *sts.pem* or *sts.cer* depending on the Save as type setting) into the **File name** box.
- 9 Click **Save** and confirm the success message.

## Listing all Certificates in a Keystore

To retrieve the alias, execute these steps:

- 1 Open a command prompt and navigate to the directory where the keystore is located.
- 2 Type `keytool` and press **Enter**. If you receive the message that `keytool` is not recognized, type the following command and press **Enter**:  
`set path=%path%; "RM_Install\Common Tools ###.#\jre\#.#\bin"`



### NOTE

- Replace `RM_Install` with the path to the Dimensions RM directory, e.g. `C:\Program Files\Open Text\Dimensions 25.2 (13)`.
- Replace `###.#` with the Common Tools version number, e.g. `2.3.0.0`.
- Replace `##` with the Java version number, e.g. `11.0`.

The complete set command may look like this:

```
set path=%path%; "C:\Program Files\Open Text\Dimensions
12.12\Common Tools 2.3.0.0\jre\11.0\bin"
```

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



### NOTE

- Replace `Keystore` with the path to the desired keystore. If the path contains spaces, surround the path with double quotes.
- Replace `StorePassword` with the password for the keystore.

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

```
keytool -list -v -keystore sample-ssl.jks -storepass serena
>certs.txt
```

- 4 Type `notepad certs.txt` and press **Enter**. This opens the file `certs.txt` in Notepad. The file `certs.txt` contains detailed information about all certificates in the keystore.

## Retrieving the Alias from a PFX File

When importing the certificate into the Dimensions RM 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\Open Text\Dimensions 25.2 (13)`.
- Replace `#.#.#.#` with the Common Tools version number, e.g. `2.3.0.0`.
- Replace `#.#` with the Java version number, e.g. `11.0`.

The complete set command may look like this:

```
set path=%path%; "C:\Program Files\Open Text\Dimensions
12.12\Common Tools 2.3.0.0\jre\11.0\bin"
```

- 3 Type the following command (all on one line) and press **Enter**:  
`keytool -list -v`  
`-keystore PfxCertificate -storepass PfxPassword >pfx.txt`

**NOTE**

- Replace *PfxCertificate* with the file name of your PFX certificate. If the file name contains spaces, surround the file name with double quotes.
- Replace *PfxPassword* with the password for the PFX certificate. If you exported the certificate as described in chapter ["Exporting Certificates to PFX Format from the Management Console,"](#) use the password you specified on export.

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

```
keytool -list -v
-keystore MyCertificate.pfx -storepass topsecret >certs.txt
```

- 4 Type `notepad pfx.txt` and press **Enter**. This opens the file `pfx.txt` in Notepad.
- 5 Locate the line starting with **Alias name** and write down the value. In this example, the alias name is `1: Alias name: 1`

## Retrieving Root CA and Intermediate CA Certificate Files

### Retrieving From a Certificate

The system certificate manager typically manages many certificates. The following steps show how to extract a certificate for both PFX and CER certificates. If there are issues, please check your corporate system administrator.

A certificate path may look like this:

- Root CA
  - Intermediate CA

- Server

There may be several intermediate CAs in a certificate. If the intermediate CA files are required, all must be exported.

### Retrieving Root CA and Intermediate CA Certificate Files from a PFX File

PFX files must be opened in the Certificate Manager.

#### To open a PFX certificate in the Certificate Manager, execute these steps:

- 1 Open a command prompt.
- 2 Type `certmgr` and press **Enter**. This starts the Certificate Manager.
- 3 Locate the certificate in the tree. A common location may be `Personal | Certificates`.

If you cannot find the certificate, you need to (temporarily) import it by executing these steps:

- a Right-click the **Personal** folder. In the shortcut menu, point to **All Tasks**, and then select **Import....** This opens the **Certificate Import Wizard**.
  - b Click **Next**.
  - c Click **Browse....**
  - d From the file filter box, select **Personal Information Exchange (\*.pfx;\*.p12)**.
  - e Select the PFX file and click **Open**.
  - f Click **Next**.
  - g In the **Password** box, type the current password for the PFX file.
  - h Click **Next**.
  - i Click **Next**.
  - j Click **Finish** to import the file and confirm the success message.
  - k In the tree, expand **Personal**, then select **Certificates**.
- 4 Double-click the Certificate. This opens the **Certificate** dialog. Continue with step 2 in chapter ["Retrieving from a CER File" on page 441](#).

### Retrieving from a CER File

The following steps describe how to retrieve root CA and intermediate CA certificates from a server certificate file in CER format. Depending on your certificate, there may be no root CA and/or intermediate CA certificates.

#### To retrieve root CA and intermediate CA certificate files from a CER file, do the following:

- 1 Double-click the CER file. This opens the **Certificate** dialog.
- 2 Select the **Certification Path** tab.
- 3 If you see only one entry (your server name), there are no root CA and intermediate CAs. Skip all further steps.
- 4 Select the top certificate (this is the root CA).

- 5 Click **View Certificate**. This opens the selected certificate.
- 6 Select the **Details** tab.
- 7 Click **Copy to File....** This opens the **Certificate Export Wizard**.
- 8 Click **Next**.
- 9 Select the export format, e.g. **DER-encoded binary X.509 (.CER)**.
- 10 Click **Next**.
- 11 Click **Browse...** to specify the path/file name to which you want to export the certificate.
- 12 Click **Next**.
- 13 Click **Finish** and confirm the success message.
- 14 Click **OK** to close the certificate.
- 15 If there are certificates between the root CA certificate and the server certificate, select each of them and execute steps 5-14.

## Importing Root and Intermediate CA into Local Certificate Store

**To import a root CA certificate and/or an intermediate CA certificate in CER format, do the following:**

- 1 On the server, open a command prompt.
- 2 Enter **mmc** and press **Enter** to start the Microsoft Management Console.
- 3 From the **File** menu, select **Add/Remove Snap-in...** or press **Ctrl+M**.
- 4 From the list **Available snap-ins**, select **Certificates**.
- 5 Click **Add**.
- 6 In the **Certificates snap-in** dialog, do the following:
  - a Select **Computer account**.
  - b Click **Next**.
  - c Ensure that option **Local computer: (the computer this console is running on)** is selected.
  - d Click **Finish**.
- 7 Click **OK**.
- 8 Expand **Certificates (Local Computer)**.
- 9 To import a **root CA certificate**, do the following:
  - a Right-click **Trusted Root Certification Authorities**. This opens a shortcut menu.

- b** Point to **All Tasks**, then select **Import....** This opens the **Certificate Import Wizard**.
  - c** Click **Next**.
  - d** Click **Browse....** This opens the **Open** dialog.
  - e** In the file filter box, select **X.509 Certificate (\*.cer;\*.crt)**.
  - f** Select the CER certificate and click **Open**.
  - g** Click **Next**.
  - h** Click **Next**.
  - i** Click **Finish** and confirm the success message.
- 10** To import an **intermediate CA certificate**, do the following:
- a** Right-click **Intermediate Certification Authorities**. This opens a shortcut menu.
  - b** Point to **All Tasks**, then select **Import....** This opens the **Certificate Import Wizard**.
  - c** Click **Next**.
  - d** Click **Browse....** This opens the **Open** dialog.
  - e** In the file filter box, select **X.509 Certificate (\*.cer;\*.crt)**.
  - f** Select the CER certificate and click **Open**.
  - g** Click **Next**.
  - h** Click **Next**.
  - i** Click **Finish** and confirm the success message.



# Appendix B

---

## Database Security

Overview	446
Oracle Database Security	446
MS SQL Server Database Security	457
PostgreSQL Database Security	463

## Overview

This chapter provides the procedures to configure your database to provide more security. Note that the procedures described may or may not work on your environment.

## Oracle Database Security

### Shall I use Transport Encryption or Native Network Encryption?

Transport encryption is safer than native network encryption, but requires configuration on the client machines.

The following overview shows the differences between those encryptions:

**Transport Encryption:** (see chapter ["Transport Encryption with Oracle" on page 446](#))

- ++ Very secure
- + Security standard compliant
- + Strong authentication when using PKI certificates
- Uses a certificate, which needs to be updated regularly
- Changes on client machines are necessary

**Native Encryption:** (see chapter ["Native Network Encryption with Oracle" on page 452](#))

- + Easy to configure
- + No changes for client machines necessary
- + No certificate required
- Not as secure as Transport Encryption; it allows server impersonation for example



**CAUTION!** You should only use one encryption method (in this case: transport encryption). If you enable both, transport encryption **and** native encryption, you will get the ORA-12696 Double Encryption Turned On error for databases older than 19c.

### Transport Encryption with Oracle

Transport encryption requires that some steps are done on the database machine while other steps are done on the Dimensions RM application server and those machines on which you have the Dimensions RM admin client tools (such as RM Manage) installed.

**Execute the following steps:**

- 1 Open a remote session to the Dimensions RM application server.
- 2 Stop all Dimensions RM related services in this order:

- Dimensions RM SyncEngine and any other SyncEngine service
- Dimensions RM Common Tomcat
- Dimensions RM Dimensions RM Pool Manager
- Dimensions RM ALF Event Emitter
- Dimensions RM E-Mail Notification Service



**IMPORTANT!** While the services are shut down, users cannot use Dimensions RM. If there are other web applications running on Dimensions RM Common Tomcat, users of those applications will also be unable to work.

- 3 Execute the steps described in chapter "[Database Server Configuration](#)" on page 447.
- 4 Execute the steps described in chapter "[Dimensions RM Application Server and Admin Client Configuration](#)" on page 450.
- 5 Start the services you shut down in step 2 in this order:
  - Dimensions RM Dimensions RM Pool Manager
  - Dimensions RM Common Tomcat
  - Dimensions RM ALF Event Emitter
  - Dimensions RM E-Mail Notification Service
  - Dimensions RM SyncEngine and any other SyncEngine service
- 6 If you have client machines running the Dimensions RM admin client tools (such as RM Manage), execute the steps described in chapter "[Dimensions RM Application Server and Admin Client Configuration](#)" on page 450.

### **Database Server Configuration**



**CAUTION!** Before you start, ensure that all services related to Dimensions RM have been stopped (see chapter "[Transport Encryption with Oracle](#)" on page 446).



**IMPORTANT!** The following steps will use the placeholder `$ORACLE_HOME`. In those steps you need to replace `$ORACLE_HOME` with the actual path of your Oracle home directory. e.g. `C:\app\ORACLEAdmin\product\12.1.0\dbhome_1`

#### **To configure Oracle to use transport encryption, execute these steps:**

- 1 Log in (e.g. by a Remote Desktop connection) to the Oracle database server.
- 2 Open a command prompt.
- 3 Change to your Oracle home directory, e.g.  
`C:\app\ORACLEAdmin\product\12.1.0\dbhome_1.`
- 4 Type the following command and press **Enter**: `md tns_wallet`
- 5 Type the following command (all on one line) and press **Enter**:  
`orapki wallet create`

```
-wallet "$ORACLE_HOME\tns_wallet" -pwd myPass -auto_login
```

**NOTE**

- Replace *\$ORACLE\_HOME* with the full path to your Oracle home directory.
- Replace *myPass* with your preferred password and take a note of that password.

- 6 Assign a certificate to the wallet.

**To create a self-signed certificate:**

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

```
orapki wallet add -wallet "$ORACLE_HOME\tns_wallet" -pwd myPass
-sign_alg sha256 -dn "CN=dbcert" -keysize 2048 -self_signed
-validity 180
```

**NOTE**

- Replace *\$ORACLE\_HOME* with the full path to your Oracle home directory.
- Replace *myPass* with the password you specified in step 4.
- Change the validity (180 in the command above) to your preferred value.

**To use an existing certificate in CER format, execute these steps:**

- a Retrieve the root CA certificate and all Intermediate CA certificate from the certificate as described in chapter ["Retrieving Root CA and Intermediate CA Certificate Files"](#) on page 440.



**TIP** If you have more than one intermediate CA certificate, number them as you need to import them in that order as they are in the certificate.

- b To import the root certificate, type the following command (all on one line) and press **Enter**:

```
orapki wallet add -wallet "$ORACLE_HOME\tns_wallet" -pwd myPass
-trusted_cert -cert C:\temp\Root.cer
```

**NOTE**

- Replace *\$ORACLE\_HOME* with the full path to your Oracle home directory.
- Replace *myPass* with the password you specified in step 4.
- Replace the certificate path to match your environment.

- c To import an intermediate CA certificate, type the following command (all on one line) and press **Enter**:

```
orapki wallet add -wallet "$ORACLE_HOME\tns_wallet" -pwd myPass
-trusted_cert -cert C:\temp\Intermediate1.cer
```

**NOTE**

- Replace *\$ORACLE\_HOME* with the full path to your Oracle home directory.
- Replace *myPass* with the password you specified in step 4.
- Replace the certificate path to match your environment.

**d** Repeat step c for any other intermediate CA certificate.

**e** To import the trusted certificate, type the following command (all on one line) and press **Enter**:

```
orapki wallet add -wallet "$ORACLE_HOME\tns_wallet" -pwd myPass
-trusted_cert -cert c:\temp\Mycert.cer
```

**7 If you created a self-signed certificate in step 6:**

Export the certificate as a file by typing the following command (all on one line) followed by **Enter**:

```
orapki wallet export -wallet "$ORACLE_HOME\tns_wallet" -pwd myPass
-dn "CN=dbcert" -cert C:\temp\db-export-certificate.cer
```

**NOTE**

- Replace *\$ORACLE\_HOME* with the full path to your Oracle home directory.
- Replace *myPass* with the password you specified in step 4.
- Replace the certificate path to match your environment.

**8** Retrieve the exported certificate (and root CA and intermediate CA certificates if you used a certificate in PFX format) for Dimensions RM application server and admin client tools configuration.

**9** Navigate to the `listener.ora` file, which is located in `$ORACLE_HOME\NETWORK\ADMIN`.

**10** Open the `listener.ora` file with Notepad.

**11** Add the following line to the address list section:

```
(ADDRESS = (PROTOCOL = TCPS)(HOST = 0.0.0.0)(PORT = 1777))
```



**NOTE** Replace 0.0.0.0 with the actual hostname/IP value of your environment

Replace 1777 with the port number you wish to use with your environment.

**12** Save the file.

**13** Restart the Oracle Listener service.

## Dimensions RM Application Server and Admin Client Configuration



**CAUTION!** Before you start, ensure that you executed the previous steps (see chapter "Transport Encryption with Oracle" on page 446).



**IMPORTANT!** The following steps will use the placeholder `$ORACLE_HOME`. In those steps you need to replace `$ORACLE_HOME` with the actual path of your Oracle home directory. e.g. `C:\app\ORACLEAdmin\product\12.1.0\dbhome_1`

### To configure Dimensions RM to use transport encryption for Oracle database connections, execute these steps:

- 1 Log in (e.g. by a Remote Desktop connection) to the Dimensions RM application server.

If your Oracle database is running on the same machine as your Dimensions RM server, continue with step 7.

- 2 Open a command prompt.
- 3 Change to your Oracle home directory, e.g.  
`C:\app\ORACLEAdmin\product\12.1.0\dbhome_1`.
- 4 Type the following command and press **Enter**: `md tns_wallet`
- 5 Type the following command (all on one line) and press **Enter**:  
`orapki wallet create`  
`-wallet "$ORACLE_HOME\tns_wallet" -pwd myPass -auto_login_local`



#### NOTE

- Replace `$ORACLE_HOME` with the full path to your Oracle home directory.
- Replace `myPass` with your preferred password and take a note of that password.

- 6 Import the certificate(s) from the database server.
  - a If there is a root certificate, type the following command (all on one line) and press **Enter**:

```
orapki wallet add -wallet "$ORACLE_HOME\tns_wallet" -pwd myPass
-trusted_cert -cert C:\temp\Root.cer
```



#### NOTE

- Replace `$ORACLE_HOME` with the full path to your Oracle home directory.
- Replace `myPass` with the password you specified in step 4.
- Replace the certificate path to match your environment.

- b If there is at least one intermediate CA certificate, type the following command (all on one line) and press **Enter**:

```
orapki wallet add -wallet "$ORACLE_HOME\tns_wallet" -pwd myPass
-trusted_cert -cert C:\temp\Intermediate1.cer
```

**NOTE**

- Replace *\$ORACLE\_HOME* with the full path to your Oracle home directory.
- Replace *myPass* with the password you specified in step 4.
- Replace the certificate path to match your environment.

**c** Repeat step b for any other intermediate CA certificate.

**d** To import the database server certificate, type the following command (all on one line) and press **Enter**:

```
orapki wallet add -wallet "$ORACLE_HOME\tns_wallet" -pwd myPass
-trusted_cert -cert C:\temp\db-export-certificate.cer
```

**NOTE**

- Replace *\$ORACLE\_HOME* with the full path to your Oracle home directory.
- Replace *myPass* with the password you specified in step 4.
- Replace the certificate path to match your environment.

**7** Navigate to the `sqlnet.ora` file, which is located in `$ORACLE_HOME\NETWORK\ADMIN`.

**8** Open the `sqlnet.ora` file with Notepad.

**9** Add the following text:

```
WALLET_LOCATION =
  (SOURCE =
    (METHOD = FILE)
    (METHOD_DATA =
      (DIRECTORY = $ORACLE_HOME\tns_wallet)
    )
  )
SSL_CLIENT_AUTHENTICATION = FALSE
SSL_CIPHER_SUITES=(SSL_RSA_WITH_AES_256_CBC_SHA,
SSL_RSA_WITH_3DES_EDE_CBC_SHA)
```



**NOTE** Replace *\$ORACLE\_HOME* with the full path to your Oracle home directory.

**10** For `SQLNET.AUTHENTICATION_SERVICES`, add the **TCPS** protocol, so it might look like this: `SQLNET.AUTHENTICATION_SERVICES = (TCPS,NTS)`

**11** Save the file.

**12** Navigate to the `tnsnames.ora` file, which is located in `$ORACLE_HOME\NETWORK\ADMIN`

Add the following:

```
RM_SSL =
  (DESCRIPTION=
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCPS) (HOST = 0.0.0.0) (PORT = 1777))
    )
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = RM)
    )
  )
)
```



#### NOTE

- Replace 0.0.0.0 with the actual hostname/IP value of your environment
- Replace 1777 with the port number you wish to use with your environment.

## Native Network Encryption with Oracle

To configure native network encryption, execute these steps:

- 1 Locate your `sqlnet.ora` configuration file. Usually you find it under `product\<version>\dbhome_1\NETWORK\ADMIN`, e.g. `C:\app\ORACLEAdmin\product\12.1.0\dbhome_1\NETWORK\ADMIN`.

- 2 Open the `sqlnet.ora` file with Notepad.

- 3 Add the following lines:

```
SQLNET.ENCRYPTION_SERVER = required
SQLNET.ENCRYPTION_TYPES_SERVER = (AES256)
```

- 4 Save the file.

- 5 To verify if the configuration change is successful, do the following:

- a Open a command prompt.
- b Type `sqlplus` and press **Enter**.
- c Log in as an administrative user (e.g. `sys` or `ICDBA`)
- d Execute the following command:
 

```
select network_service_banner from v$session_connect_info where
sid in (select distinct sid from v$mystat);
```
- e Verify that the output is similar to this:

```
NETWORK_SERVICE_BANNER
```

```
-----
-----
```

```
Windows NT TCP/IP NT Protocol Adapter for 64-bit Windows: Version
12.1.0.1.0 - Production
```

```
Authentication service for 64-bit Windows: Version 12.1.0.1.0 -
Production
```

```
NTS Authentication service adapter for 64-bit Windows: Version
2.0.0.0.0 - Production
```

```
Encryption service for 64-bit Windows: Version 12.1.0.1.0 -
Production
```

```
AES256 Encryption service adapter for 64-bit Windows: Version
12.1.0.1.0 - Production
```

```
NETWORK_SERVICE_BANNER
```

```
-----
```

```
Crypto-checksumming service for 64-bit Windows: Version 12.1.0.1.0
- Production
```

```
6 rows selected.
```

## Transparent Data Encryption with Oracle

Transparent Data Encryption (TDE) encrypts the database files and backups (when you create them after encrypting the database) as to avoid that data can be stolen by retrieving the database file or backup. During the process, you need to create an Oracle wallet. It is essential to store its password in a safe location. For enabling TDE you need the following:

- Access to the Dimensions RM server as an administrator
- Oracle SqlPlus
- User name and password of a Dimensions RM administrator user
- The password of the ICDBA user



**IMPORTANT!** During the process, Dimensions RM and any other web application running on the same server will not be available to users.

Enabling TDE consists of these steps:

- 1 Prepare for TDE:
  - a Stop Dimensions RM services.
  - b Create a backup with RM Manage as to be able to restore the database in case of issues.
- 2 Enabling TDE:
  - a Create a Certificate

- b** Backup the master key
  - c** Backup the certificate
  - d** Encrypt the database
- 3** Verification and Starting Dimensions RM
  - a** Verify that the database can be accessed
  - b** Start Dimensions RM services

### ***Preparing for Transparent Data Encryption***



**IMPORTANT!** The following steps are to ensure that there is no database access during the encryption process and that you are able to restore the data in case encryption fails.

To prepare for Transparent Data Encryption:

- 1** Open a Remote Desktop connection to the Dimensions RM server.
- 2** Stop the following services in this order:
  - Dimensions RM SyncEngine and any other SyncEngine services
  - Dimensions RM Common Tomcat
  - Dimensions RM Dimensions RM Pool Manager
  - Dimensions RM ALF Event Emitter
  - Dimensions RM E-Mail Notification Service
- 3** Start RM Manage.
- 4** Create a backup of your database as described in chapter ["Restoring an Instance Account under MS SQL Server"](#) on page 192. This backup will **not** be encrypted.
- 5** Close RM Manage.
- 6** Open a command prompt as an administrator and execute the following command:  
`taskkill /f /im rmLicenseAgent.exe`  
Alternatively, you can terminate all rmLicenseAgent.exe instances in Task Manager.

### ***Enabling Transparent Data Encryption***



**IMPORTANT!** Before you execute the steps below, ensure that you executed the steps described in chapter ["Preparing for Transparent Data Encryption"](#) on page 461.

#### **To enable Transparent Data Encryption (TDE):**

- 1** Log in (e.g. by a Remote Desktop connection) to the Oracle database server.
- 2** Open a command prompt.

- 3 Change to your Oracle home directory, e.g.  
`C:\app\ORACLEAdmin\product\12.1.0\dbhome_1.`
- 4 Type the following command and press **Enter**: `md tde_wallet`
- 5 Type the following command (all on one line) and press **Enter**:  
`orapki wallet create`  
`-wallet "$ORACLE_HOME\tde_wallet" -pwd myPass -auto_login_local`

**NOTE**

- Replace `$ORACLE_HOME` with the full path to your Oracle home directory.
- Replace `myPass` with your preferred password and take a note of that password.

- 6 Type `sqlplus` and press **Enter**.
- 7 Log in as an administrator, e.g. `sys@RM as sysdba`  
Change the database from `RM` to your database name.
- 8 Type the following commands and hit **Enter**:

```
ALTER SYSTEM SET
WALLET_ROOT='C:\app\ORACLEAdmin\product\12.1.0\dbhome_1\tde_wallet'
SCOPE=SPFILE SID='*';
```



**NOTE** Replace the path with the path matching your environment.

```
ALTER SYSTEM SET TDE_CONFIGURATION="KEYSTORE_CONFIGURATION=FILE"
SCOPE=BOTH SID='*';

ADMINISTER KEY MANAGEMENT CREATE KEYSTORE IDENTIFIED BY myStorePass;
```



**NOTE** Replace `myStorePass` with your preferred password and take a note of that password. Use this password for all commands that use `myStorePass`.

```
ADMINISTER KEY MANAGEMENT CREATE AUTO_LOGIN KEYSTORE FROM KEYSTORE
'C:\app\ORACLEAdmin\product\12.1.0\dbhome_1\tde_wallet' IDENTIFIED
BY myStorePass;
```

**NOTE**

- Replace the path with the path matching your environment.
- Replace `myStorePass` with the keystore password.

```
ADMINISTER KEY MANAGEMENT SET KEYSTORE OPEN IDENTIFIED BY
myStorePass;
```



**NOTE** Replace *myStorePass* with your preferred password and take a note of that password. Use this password for all commands that use *myStorePass*.

```
SELECT STATUS FROM V$ENCRYPTION_WALLET;

ADMINISTER KEY MANAGEMENT SET KEY IDENTIFIED BY myKeyPass WITH BACKUP
USING 'key_backup';
```



**NOTE** Replace *myKeyPass* with your preferred password and take a note of that password.

```
SELECT STATUS FROM V$ENCRYPTION_WALLET;
```

```
ALTER TABLESPACE RMDEMO ENCRYPTION ONLINE USING 'AES256' ENCRYPT
FILE_NAME_CONVERT = ('RMDEMO01-30-2022-184736.DBF',
'RMDEMO01-30-2022-184736_ENC.DBF');
```



**NOTE**

- Replace the tablespace *RMDEMO* with the tablespace you wish to encrypt.
- Replace the first file name with the file name that contains the data of the table space you wish to convert.
- Replace the second file name with a new file name, reflecting the tablespace. It must be different from the first file name. To show that it contains encrypted data, we recommend to add "\_ENC" to the first file name.

- 9 Repeat the ALTER TABLESPACE command for all tablespaces you want to encrypt.
- 10 Type `exit` and press **Enter**.
- 11 Restart the database service.
- 12 Delete the unencrypted DBF files (only those that were replaced by their encrypted counterparts). For the example above, you would delete the *RMDEMO01-30-2022-184736.DBF* file.

### **Verification and Starting Dimensions RM**

- 1 Verify the functionality of Dimensions RM by executing these steps:
  - a Start RM Manage.
  - b Log in with user name and password of an administrator.
- 2 If the verification in step 1 is successful, start the following services in this order:
  - Dimensions RM Dimensions RM Pool Manager
  - Dimensions RM Common Tomcat

- Dimensions RM ALF Event Emitter (if it was running before)
- Dimensions RM E-Mail Notification Service (if it was running before)
- Dimensions RM SyncEngine and any other SyncEngine services (if these services were running before)

## MS SQL Server Database Security

- Transport Encryption with MS SQL Server

Dimensions RM can connect to Microsoft SQL Server using Transport Layer Security (TLS). A TLS connection encrypts the data and thus prevents that data transmitted through a database connection can be read by other parties. Using TLS requires a server certificate, which must match the prerequisites (see chapter "[Prerequisites](#)" on page 457). Then configure the SQL server machine(s) as described below:

- **SQL Server 2019:** see chapter "[Installing a Certificate for SQL Server 2016/2017](#)" on page 458
- **SQL Server 2016/2017:** see chapter "[Installing a Certificate for SQL Server 2019](#)" on page 459

### **Prerequisites**

To be able to use Transport Encryption, you require a certificate for the SQL Server. The certificate must meet the following conditions:

- The certificate must be issued for **Server Authentication (1.3.6.1.5.5.7.3.1)**.
- The certificate must be a legacy certificate. This means that the certificate was created using the **KeySpec** option **AT\_KEYEXCHANGE**. In most cases, the **KEY\_USAGE** property will include key encipherment (**CERT\_KEY\_ENCIPHERMENT\_KEY\_USAGE**).
- The **Subject** property of the certificate must show that the common name is either the host name (e.g. mydbserver) or the fully qualified domain name (e.g. mydbserver.mydomain.com) of the machine running SQL Server. If SQL Server is running on a failover cluster, the common name must be either the host name, or the fully qualified domain name of the virtual server and the certificate must be provisioned on all nodes in the failover cluster.
- The **Valid from** and **Valid to** properties of the certificate must define a time range for that covers the current system time.
- By default, Microsoft SQL Server does not support wildcard certificates. To use wildcard certificates, please refer to the Microsoft SQL Server documentation.
- All CA certificates (root CA and intermediate CA certificates) of the server certificate must be valid (Valid from/Valid to properties) and recognized by Windows. If any of them is not recognized, import them into the Windows Certificate Store as described in chapter "[Importing Root and Intermediate CA into Local Certificate Store](#)" on page 442.

If you do not have the root CA/intermediate CA certificate files, see chapter "[Retrieving Root CA and Intermediate CA Certificate Files](#)" on page 440 for further information.

### **Installing a Certificate for SQL Server 2016/2017**

**To install a certificate for SQL Server 2016 or 2017, do the following:**

- 1** Ensure that the certificate matches the prerequisites and is valid and recognized by Windows (see chapters "Retrieving Root CA and Intermediate CA Certificate Files" on page 440 and "Importing Root and Intermediate CA into Local Certificate Store" on page 442).
- 2** On the server, open a command prompt.
- 3** Enter **mmc** and press **Enter** to start the Microsoft Management Console.
- 4** From the **File** menu, select **Add/Remove Snap-in...** or press **Ctrl+M**.
- 5** From the list **Available snap-ins**, select **Certificates**.
- 6** Click **Add**.
- 7** 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**.
- 8** Click **OK**.
- 9** Expand **Certificates (Local Computer)**.
- 10** Expand **Personal**.
- 11** Select **Certificates**, if it exists. This lists all personal certificates and allows you to check if the certificate has been imported before.
- 12** Right-click **Personal**. This opens a shortcut menu.
- 13** Point to **All Tasks**, then select **Import...** This opens the **Certificate Import Wizard**.
- 14** Click **Next**.
- 15** Click **Browse...** This opens the **Open** dialog.
- 16** In the file filter box, select **Personal Information Exchange (\*.pfx;\*.p12)**.
- 17** Select the PFX certificate and click **Open**.
- 18** Click **Next**.
- 19** Enter the password into the **Password** box.
- 20** Select the option **Make this key exportable. This will allow you to back up or transport your keys at a later time**.
- 21** Ensure that the option **Allow this certificate to be exported** is selected.

- 22 Click **Next**.
- 23 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**.
- 24 Click **Next**.
- 25 Click **Finish** and confirm the success message.
- 26 In the tree, expand **Personal**.
- 27 Select **Certificates**.
- 28 Right-click the imported server certificate. This opens a shortcut menu.
- 29 Point to **All Tasks**, then select **Manage Private Keys**. This opens the **Permissions** dialog.
- 30 If the SQL Server service account is not listed in the **Group or user names** list, do the following:
  - a Click **Add....** This opens the **Select Users or Groups** dialog.
  - b Enter the SQL Server service account name into the **Enter the object name to select** box and click **Check Names**. This completes the user name and underlines it.
  - c Ensure that the added user is selected.
  - d Revoke **Full control**, if it is selected.
  - e Grant **Read**, if it is not selected.
  - f Click **OK**.
- 31 Restart the **SQL Server (<instance name>)** service.
- 32 If using several SQL Server machines, repeat above steps on each machine.

### ***Installing a Certificate for SQL Server 2019***

#### **To install a certificate for SQL Server 2019, do the following:**

- 1 Ensure that the certificate matches the prerequisites and is valid and recognized by Windows (see chapters ["Retrieving Root CA and Intermediate CA Certificate Files"](#) on page 440 and ["Importing Root and Intermediate CA into Local Certificate Store"](#) on page 442).
- 2 Start **SQL Server Configuration Manager**.
- 3 Expand **SQL Server Network Configuration**.

- 4 Right-click **Protocol for <instance name>**, and then select **Properties**. This opens the **Protocols for <instance name> Properties** dialog.
- 5 Select the **Certificate** tab.
- 6 Select the certificate from the **Certificate** drop-down.  
If the certificate is not available in the list, do the following:
  - a Click **Import**. This opens the **Select Certificate** wizard.
  - b From the **Select Certificate Type** section, select the option that matches your certificate file.
  - c If you are installing the certificate for a single node, click **Browse** and select certificate file. Then skip to step e.
  - d If you are installing a certificate for each node, click **Next** to list possible owner nodes. Then, select the nodes you wish to install the certificate for.
  - e Click **Next**.
  - f If required, specify the certificate password and click **Next**.
  - g Click **Next** to import the certificate.
  - h Click **Finish**.



**NOTE** After import, the certificate is not shown in the **Certificate** drop-down.

- 7 Click **OK**.
- 8 Restart the **SQL Server (<instance name>)** service.

## Transparent Data Encryption with MS SQL Server

Transparent Data Encryption (TDE) encrypts the database files and backups (when you create them after encrypting the database) as to avoid that data can be stolen by retrieving the database file or backup. During the process, you need to create a certificate. It is essential to store this certificate and its password in a safe location. For enabling TDE you need the following:

- Access to the Dimensions RM server as an administrator
- SQL Server Management Studio
- User name and password of a Dimensions RM administrator user
- The password of the ICDBA user



**IMPORTANT!** During the process, Dimensions RM and any other web application running on the same server will not be available to users.

Enabling TDE consists of these steps:

- 1 Prepare for TDE:
  - a Stop Dimensions RM services.

- b** Create a backup with RM Manage as to be able to restore the database in case of issues.
- 2** Enabling TDE:
  - a** Create a Certificate
  - b** Backup the master key
  - c** Backup the certificate
  - d** Encrypt the database
- 3** Verification and Starting Dimensions RM
  - a** Verify that the database can be accessed
  - b** Start Dimensions RM services

### ***Preparing for Transparent Data Encryption***



**IMPORTANT!** The following steps are to ensure that there is no database access during the encryption process and that you are able to restore the data in case encryption fails.

#### **To prepare for Transparent Data Encryption:**

- 1** Log in (e.g. by a Remote Desktop connection) to the Dimensions RM server.
- 2** Stop the following services in this order:
  - Dimensions RM SyncEngine and any other SyncEngine services
  - Dimensions RM Common Tomcat
  - Dimensions RM Dimensions RM Pool Manager
  - Dimensions RM ALF Event Emitter
  - Dimensions RM E-Mail Notification Service
- 3** Start RM Manage.
- 4** Create a backup of your database as described in chapter "[Restoring an Instance Account under MS SQL Server](#)" on page 192. This backup will **not** be encrypted.
- 5** Close RM Manage.
- 6** Open a command prompt as an administrator and execute the following command:
 

```
taskkill /f /im rmLicenseAgent.exe
```

 Alternatively, you can terminate all rmLicenseAgent.exe instances in Task Manager.

### ***Enabling Transparent Data Encryption***



**IMPORTANT!** Before you execute the steps below, ensure that you executed the steps described in chapter "[Preparing for Transparent Data Encryption](#)" on page 461.

#### **To enable Transparent Data Encryption (TDE):**

- 1 Start SQL Server Management Studio and log in as an administrative user, e.g. "sa".
- 2 Create master key and certificate by executing these steps:
  - a Click **New Query**. This opens a new **SQLQuery** window.
  - b Insert the following commands into the **SQLQuery** window:

```
USE master;  
  
GO  
  
CREATE MASTER KEY ENCRYPTION BY PASSWORD = '<Use strong password here>';  
  
GO  
  
CREATE CERTIFICATE MyServerCert WITH SUBJECT = 'My DEK Certificate';  
  
GO
```
  - c Specify the password and change the subject if desired.
  - d Click **Execute**.
  - e Take a note of the password.
- 3 Backup the master key and certificate by executing these steps:
  - a Click **New Query**. This opens a new **SQLQuery** window.
  - b Insert the following command into the empty **SQLQuery** window:

```
BACKUP MASTER KEY TO FILE = 'C:\db_master.key' ENCRYPTION BY  
PASSWORD = 'password'  
  
GO  
  
BACKUP CERTIFICATE MyServerCert TO FILE = 'C:\db_TDE.cer'  
WITH PRIVATE KEY  
  
(  
    FILE = 'C:\db_TDE.key',  
    ENCRYPTION BY PASSWORD = 'password'  
)  
  
GO
```
  - c Click **Execute**.
  - d Take a note of the passwords and store them in a secure place.
  - e Store db\_master.key, db\_TDE.cer, and db\_TDE.key in a secure place.
- 4 Enabling TDE by executing these steps:
  - a Click **New Query**. This opens a new **SQLQuery** window.
  - b Insert the following commands into the empty **SQLQuery** window:

```
USE RM;  
  
GO
```

```
CREATE DATABASE ENCRYPTION KEY
WITH ALGORITHM = AES_256
ENCRYPTION BY SERVER CERTIFICATE MyServerCert;
GO

ALTER DATABASE RM
SET ENCRYPTION ON;
GO
```

- c Replace the database name "RM" with the name of your database.
- d Click **Execute**.

### **Verification and Starting Dimensions RM**

- 1 Verify the functionality of Dimensions RM by executing these steps:
  - a Start RM Manage.
  - b Log in with user name and password of an administrator.
- 2 If the verification in step 1 is successful, start the following services in this order:
  - Dimensions RM Dimensions RM Pool Manager
  - Dimensions RM Common Tomcat
  - Dimensions RM ALF Event Emitter (if it was running before)
  - Dimensions RM E-Mail Notification Service (if it was running before)
  - Dimensions RM SyncEngine and any other SyncEngine services (if these services were running before)

## **PostgreSQL Database Security**

### **Transport Encryption with PostgreSQL**

Transport encryption is available if your PostgreSQL server has been compiled to support it. For further details about transport encryption, see the PostgreSQL documentation.

### **Transparent Data Encryption with PostgreSQL**

PostgreSQL does not support Transparent Data Encryption (TDE).



# Appendix C

---

## Troubleshooting

Resolving "Password May be Incorrect in Security File or Security File May Not be Found" Error	466
Unable to create ICDBA Account or RM Instance	467
RM Browser hangs when Exporting Documents	467
Exporting Documents creates DOC Files	468
Export of Requirements creates XLS Files	468
Unable to Export Dashboards	468
Word cannot open Documents	468
Unable to Save Query Results or Export Documents	469
RM Manage crashes when connecting to Dimensions CM	469
Unable to Re-login in Firefox	469
Addressing Database Performance	470

## Resolving "Password May be Incorrect in Security File or Security File May Not be Found" Error

The database encryption feature is a security measure designed to address the fact that there was a static, hard-coded password for the ICADMIN Oracle account. Before this feature was implemented, this hard-coded password was called by the Dimensions RM tools. With database password encryption, a customer can change the password for these accounts at any time, keeping them fully secure. For more information about database password encryption, see ["Database Password Encryption" on page 235](#).

There are situations in which you may receive the "Password May be Incorrect in Security File or Security File May Not be Found" error when logging in to a Dimensions RM tool. The following table describes such scenarios and provides ways you can correct the problem.

Case	Potential Problem	Troubleshooting Procedure
1	No Dimensions RM instance exists on the server.	Make sure you have a Dimensions RM instance on the server. You can test for this by selecting your database instance in RM Manage, right clicking, and selecting <b>Change User</b> from the context menu. If you get the same error message instead of a prompt to log in, then RM Manage is not able to connect to the database instance, or there is no active instance available for connection.
2	The security file could be in the wrong location.	In RM Manage, select <b>Workspace   Options</b> . Click the <b>Security</b> tab and verify the location and name of the security file.
3	The database instance might need to be updated to match the current security settings.	In RM Manage, select the database instance, right-click, and select <b>Convert Database</b> . When the database validation tool starts, select your instance and click <b>Upgrade</b> . When it prompts whether you want to recreate the stored procedures, click <b>Yes</b> .
4	The ICADMIN account could be locked.	In SQL Plus, try to log in as ICADMIN by typing the following command:  <pre>sqlplus icadmin/&lt;dummy password&gt;@&lt;database instance&gt;</pre> If Oracle returns a message that the account is locked, type the following commands to unlock it:  <pre>sqlplus icdba/icdba@&lt;database instance&gt; alter user icadmin account unlock; exit</pre>
5	The Dimensions RM or Oracle path could be wrong.	In RM Manage, select <b>Workspace   Options</b> . Click the <b>Mandatory</b> tab, and confirm that the <b>RTM_HOME</b> and <b>ORACLE_HOME</b> values are correct.

## Using CAC and Unable to Perform RM Browser User Management

Some RM Browser functions are executed using Web Services, e.g., User Management and Attribute Settings. In some CAC enabled environments, these functions could fail to return data.

The solution requires the creation of a registry entry on the RM Server:

- 1 In the following location: HKEY\_LOCAL\_MACHINE\SOFTWARE\Open Text\Dimensions RM\Environment\Default
- 2 Create registry entry: CRM\_INTERNAL\_WS\_URL
- 3 Assign the value: http://localhost:8080/
- 4 Restart **Dimensions RM Common Tomcat** service.

## Unable to create ICDBA Account or RM Instance

When using an **Oracle database with containers**, the following error messages may occur:

- **Cannot create ICDBA in CDB\$ROOT container**  
When using containers, you must configure the Oracle client's tnsnames.ora file accordingly. For further information, see chapter "64-Bit Oracle Client Installation with a Fresh Installation" in the *Dimensions RM Installation Guide*.
- **ORACLE initialization or shutdown in progress**  
If you receive this error when selecting the database container in RM Manage and trying to create the ICDBA account, this means that the container is not prepared for use. For further information, see chapter *Preparing an Existing Container for Dimensions RM* in the *Dimensions RM Installation Guide*.

## RM Browser hangs when Exporting Documents

Under certain conditions RM Browser might hang when exporting documents. After preparing the server, it might be necessary to cancel existing **winword.exe** tasks on the server.

### Windows Server is not prepared for Microsoft Office

RM Browser hangs on creating a document, if the server has not been prepared for exporting documents. For information on how to prepare your server, refer to "Support for Export/Import" in the *Dimensions RM Installation Guide*.

## Adobe Reader is installed on Windows Server

If the document contains PDF file as file attachment of a requirement, RM Browser might hang. For instructions on how to prevent Adobe Reader affecting exporting documents, see *"Using Adobe Reader on Windows Server"* in the *Dimensions RM Installation Guide*.

## A Server Upgrade has Broken Office

Server Upgrades can cause application issues, and if the Dimensions System Administrator does not have access to the server, such issues can be difficult to overcome.

Recently, a server upgrade broke the Word/Excel install such that when RM users tried the export files, the attempt would hang RM. In response to this and other issues, we are providing the System Administrator with an option to Disable Word until the larger issue is identified and corrected.

The registry setting is: **MSOFFICE\_PROCESSING**

- **FALSE** - processing is disabled
- **TRUE** - processing is enabled

## Exporting Documents creates DOC Files

If Microsoft Word is not installed on the server or the installed version is no longer supported, a DOC rather than a DOCX file will be created.

Please export using Word Document (Beta). This export option is using the Docx4j Java Library used for creating and manipulating Office OpenXML files.

## Export of Requirements creates XLS Files

The export process creates XLS files if Microsoft Excel is not installed on the server, or the installed version is not supported.

## Unable to Export Dashboards

To export dashboards, a supported version of Microsoft PowerPoint must be installed on the server.

## Word cannot open Documents

If Documents contain many lists or sub-documents (which are complete Word documents within another Word document), it is possible that Word is unable to open this document.

In this case, you can configure a Word document post processing step which executes on the Dimensions RM server and corrects these problems in the Word document. Note that this will increase export time. For further information on Word document post processing, see chapter "[Word Document Post Processing](#)" on page 491.

## Unable to Save Query Results or Export Documents

Depending on the settings of your Web browser, you may be unable to save query results or export documents. To prevent this problem, disable the pop-up blocker and allow Dimensions RM as an allowed site.

For Internet Explorer, follow these steps:

- 1 In Internet Explorer, select **Tools | Internet Options**.
- 2 In the **Internet Options** dialog, click the **Security** tab.
- 3 On the **Security** tab, click **Custom Level**. The **Security Settings** dialog opens.
- 4 Under **Downloads**, enable the following options:
  - **Automatic prompting for file downloads**
  - **File download**
  - **Font download**
- 5 Under **Miscellaneous**, disable the **Use Pop-up Blocker** option.

## RM Manage crashes when connecting to Dimensions CM

This issue occurs if the Dimensions CM Client version is not compatible with Dimensions RM. For a list of supported Dimensions CM clients, see the platform matrix at <https://www.microfocus.com/documentation/dimensions-rm/>.

## Unable to Re-login in Firefox

When using Firefox and a login name or password that has non-ASCII characters (e.g. Chinese characters or German umlauts), users cannot login in the provided login popup dialog. The issue that non-ISO-8859-1 characters are not supported is tracked by the Firefox team as bug #41489.

# Addressing Database Performance

## For all Supported Databases

Dimensions RM Database Engineers are focused on improving the User Experience, and that includes improving database performance.

Regular database maintenance is also crucial for maintaining optimal performance. This involves developing a regularly scheduled maintenance plan, which includes implementing actions from the official database documentation.

## MS SQL Server Performance Issues

### General Maintenance



**IMPORTANT! SQL Server requires regular, qualified maintenance. to maintain Dimensions RM performance.**

The maintenance plan must include recommended steps from the official documentation:

<https://learn.microsoft.com/en-us/sql/relational-databases/indexes/reorganize-and-rebuild-indexes?view=sql-server-ver16>

- Very important for RM performance: "Optimize index maintenance to improve query performance and reduce resource consumption."
- SQL indexes are one of the greatest resources when it comes to performance gain, however, they degrade over time. SQL Server has a **Rebuild Index Task** (Maintenance Plan), which should be run monthly or quarterly, depending on database load.

### SQL Server Browser Service

When using SQL Server with named instances or SQL Server Express, the **SQL Server Browser** service must be active.

**To activate the SQL Server Browser service, execute the following steps:**

- 1 Connect to the machine running SQL Server.
- 2 Open a command prompt.
- 3 Type `services.msc` and press **Enter**.
- 4 Double-click the **SQL Server Browser** service.
- 5 Ensure that the **Startup type** box shows **Automatic**.
- 6 If the **Apply** button is enabled, click **Apply**.
- 7 If the **Start** button is enabled, click **Start**.
- 8 Click **OK**.

# RM Import Designer Examples

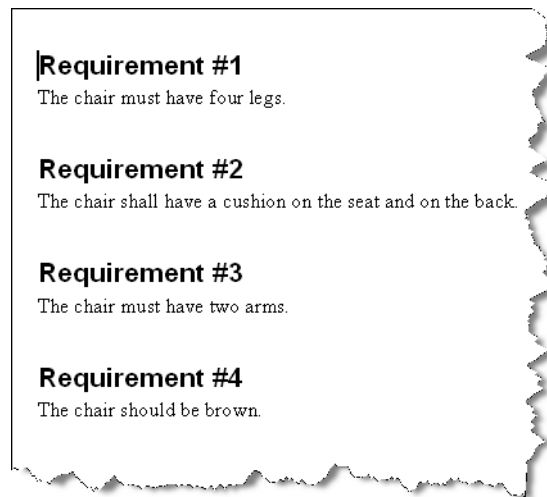
Overview	472
Begin and End Keyword	472
Entire Table with a Keyword is the Requirement	474
Table Option with Every Row	475
Section Option with Keywords	477
Heading Styles	479
Capturing Title and Description with No Title Rule	480
Capturing Title and Description with Title Rule	482

## Overview

This appendix contains examples of Word documents and explains how their structure determines how you set up templates for them in RM Import Designer. It also contains illustrations of how the document looks in Document View in RM Browser after you import it using RM Import.

## Begin and End Keyword

In this example, all four requirements are captured, because when the keyword you typed under **Begin Pattern** is found and the end of the chapter is reached, the requirement is captured, even if the keyword you typed under **End Pattern** is not at the end of the chapter.

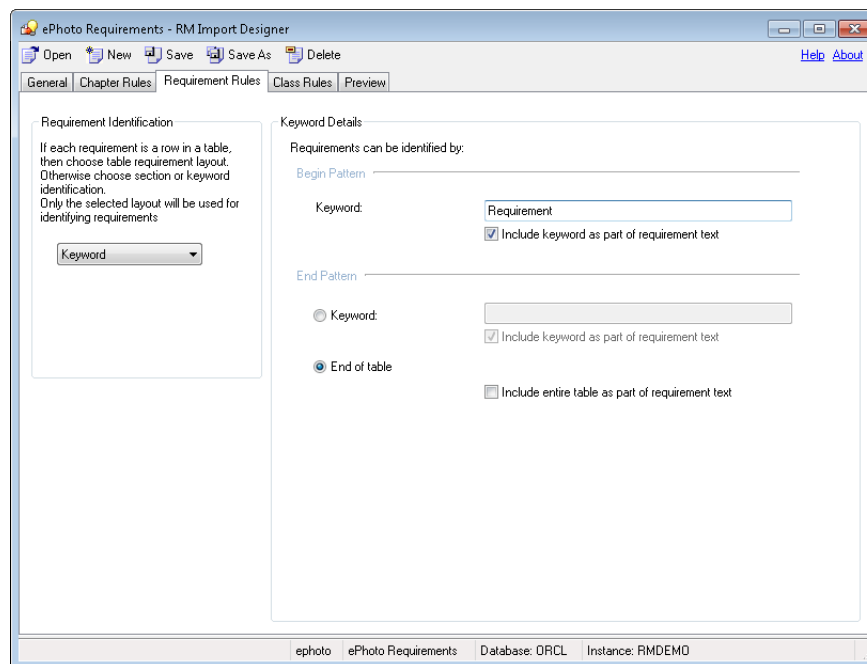




## Entire Table with a Keyword is the Requirement

In this example, the entire table is captured because the **End of table** option was selected in the **End Pattern** group, and the **Include entire table as part of requirement text** check box was selected.

Requirement Title:	Limited Documentation
<b>Benefits:</b>	1. Limited training shall be required to use product.
<b>Proofs:</b>	1. The ePhoto system uses online Help so that no guides other than a "Getting Started" Guide needs to be supplied. This has proven to be adequate according to customer feedback. 2. The product contains embedded Help so the customer can do basic tasks with no online Help or guide at all. 3. The product uses a standard Windows user interface, so the learning curve is diminished.
<b>Constraints:</b>	<None>



1.1 Limited Documentation

Propose Refresh Edit Print

Category: RMDEMO

Standard Attributes

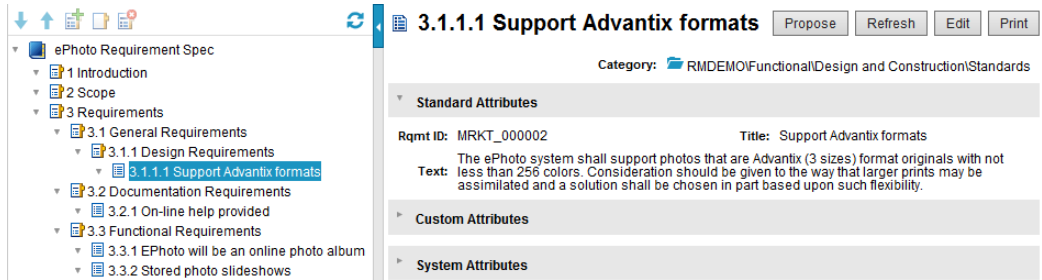
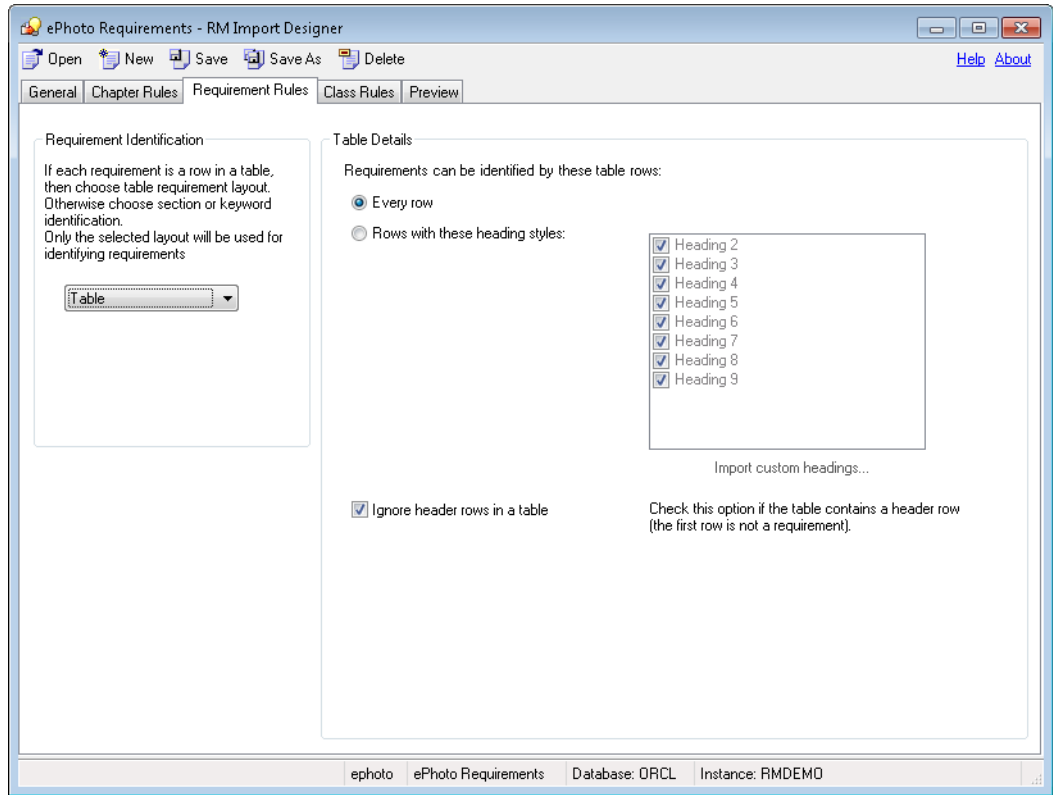
Rqmt ID: MRKT\_000041 Title: Limited Documentation

Requirement Title:	Limited Documentation
<b>Benefits:</b>	1. Limited training shall be required to use product.
<b>Proofs:</b>	1. The ePhoto system uses online Help so that no guides other than a "Getting Started" Guide needs to be supplied. This has proven to be adequate according to customer feedback. 2. The product contains embedded Help so the customer can do basic tasks with no online Help or guide at all. 3. The product uses a standard Windows user interface, so the learning curve is diminished.
<b>Constraints:</b>	<None>

## Table Option with Every Row

In this example, the title is captured because the title is in the third column of the tables, and on the **Class Rules** tab, for the **Title** attribute, **3** was typed in the **Keyword or a column number** box under **Attribute Rule**.

3 REQUIREMENTS			
<b>3.1 General Requirements</b>			
<b>3.1.1 Design Requirements</b>			
#	Rqmt ID	Title	Text
3.1.1.1	MRKT_000002	Support Advantix formats	The ePhoto system shall support photos that are Advantix (3 sizes) format originals with not less than 256 colors. Consideration should be given to the way that larger prints may be assimilated and a solution shall be chosen in part based upon such flexibility.
<b>3.1.2 Documentation Requirements</b>			
#	Rqmt ID	Title	Text
3.1.2.1	MRKT_000007	On-line help provided	The ePhoto system shall make the use of on-line help so that no documentation other than a "Getting Started" guide needs to be supplied.
<b>3.1.3 Functional Requirements</b>			
#	Rqmt ID	Title	Text
3.1.3.1	MRKT_000001	EPhoto will be an online photo album	The ePhoto system shall enable the user to browse an on-line photo album. It shall look and feel like an electronic photo album, just like the one on the coffee table.
3.1.3.1	MRKT_000004	Stored photo	The ePhoto system shall provide the ability to create slides for



## Section Option with Keywords

In this example, every paragraph containing the specified keywords is captured as a requirement.

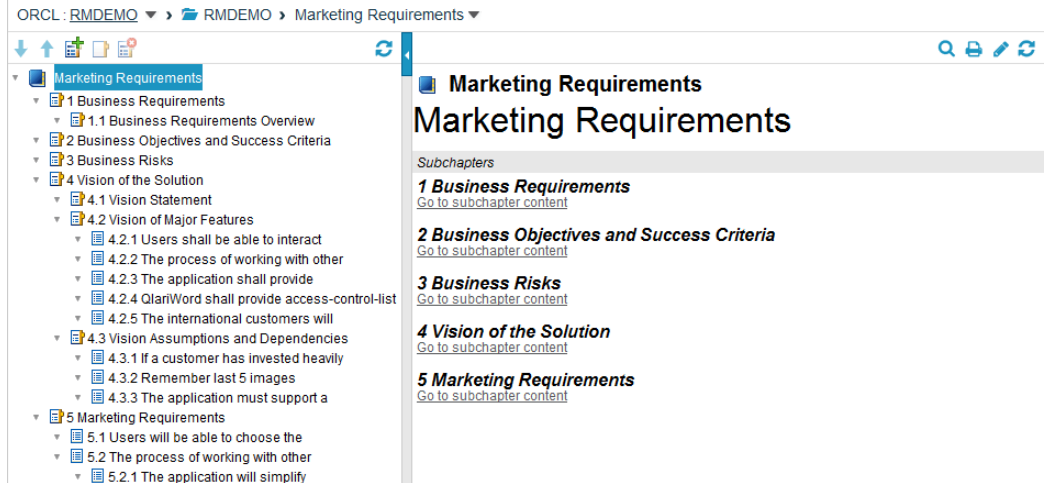
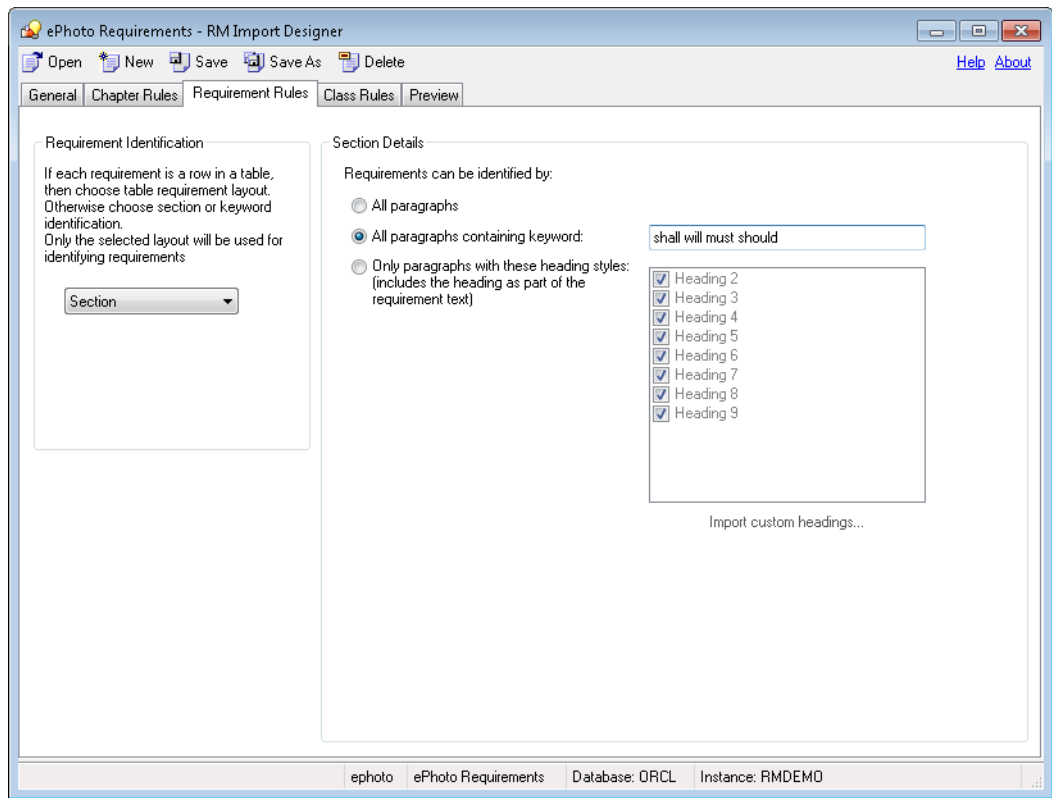
- The process of working with other shall be made easier by using document workspaces.
- The application shall provide as part of the GUI a means for users to check for updated versions of files, confirm if team members are online, view lists of related files, and view file properties.
- QlariWord shall provide access-control-list management (ACLM) for all documents.
- The application must support a spellchecker and grammar checker.

**4.3. Vision Assumptions and Dependencies**

- The international customers will require QlariWord to support their local language.
- If a customer has invested heavily in Word, QlariWord must be able to communicate with it bi-directionally.

**5. Marketing Requirements**

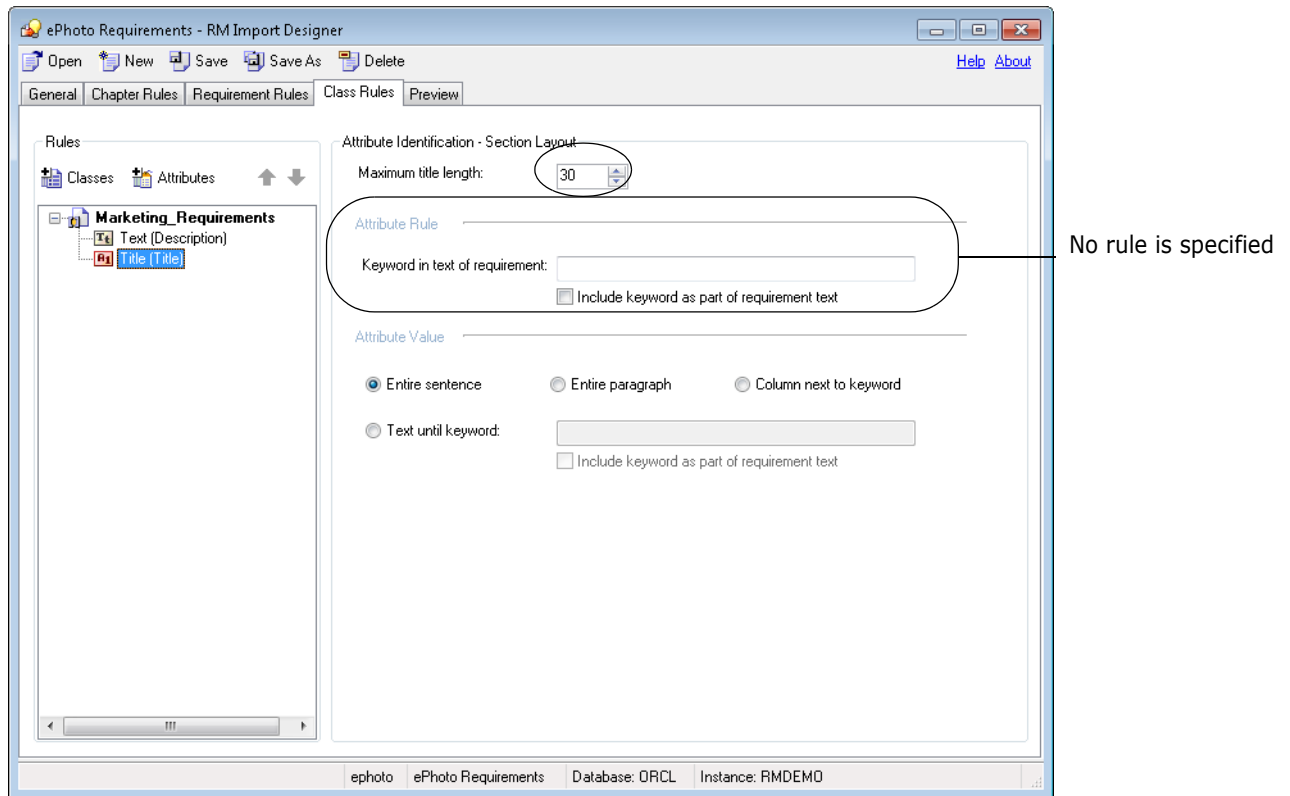
Req. #	Description
5.1.	Users will be able to choose the language they wish to work in. The default will be U.S. English.
5.2.	The process of working with other shall be made easier by using document workspaces.
5.3.	The application will simplify the task of working with others to co-author, edit, and review files.
5.4.	The application must provide as part of the GUI a means for users to check for updated versions of files, confirm if team members are online, view lists of related files, and view file properties.





## Capturing Title and Description with No Title Rule

When you add a class to the Class Rules tab in RM Import Designer, the Title and Description attributes, along with the mandatory attribute, are added to the class rules. You can specify a rule for each of these attributes that indicates how the values should be identified and captured from the Word document. These rules are optional. For attributes other than Title and Description, if no rules are specified, default values are used. The following illustration shows the case where the **Attribute Rule** field is empty; thus there is no rule.

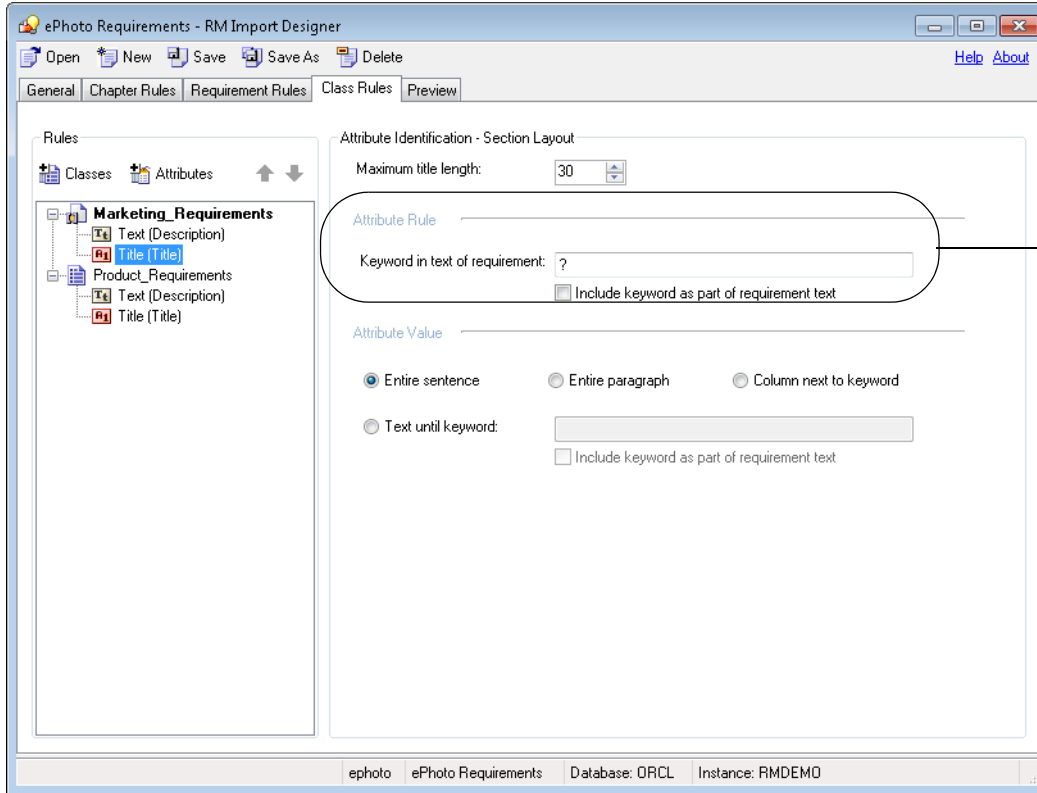


The screenshot displays a requirements management interface. On the left, a tree view shows a hierarchy of requirements. The selected requirement is '3.1.3.3 Runs on "standard" home PC'. The right pane shows the details for this requirement. The 'Text' field contains the full description: 'The ePhoto system shall be accessible to the user from a regular home PC environment running standard Windows software. It is envisaged that this is a software-only application from the user's perspective.' The 'Title' field shows the truncated title: '3.1.3.3 Runs on "standard" home'. A callout box points to the text field, stating: 'The **Title** is duplicated in the **Text** field. Note that the **Title** is truncated due to the default rule that the maximum title length is 30 characters.'

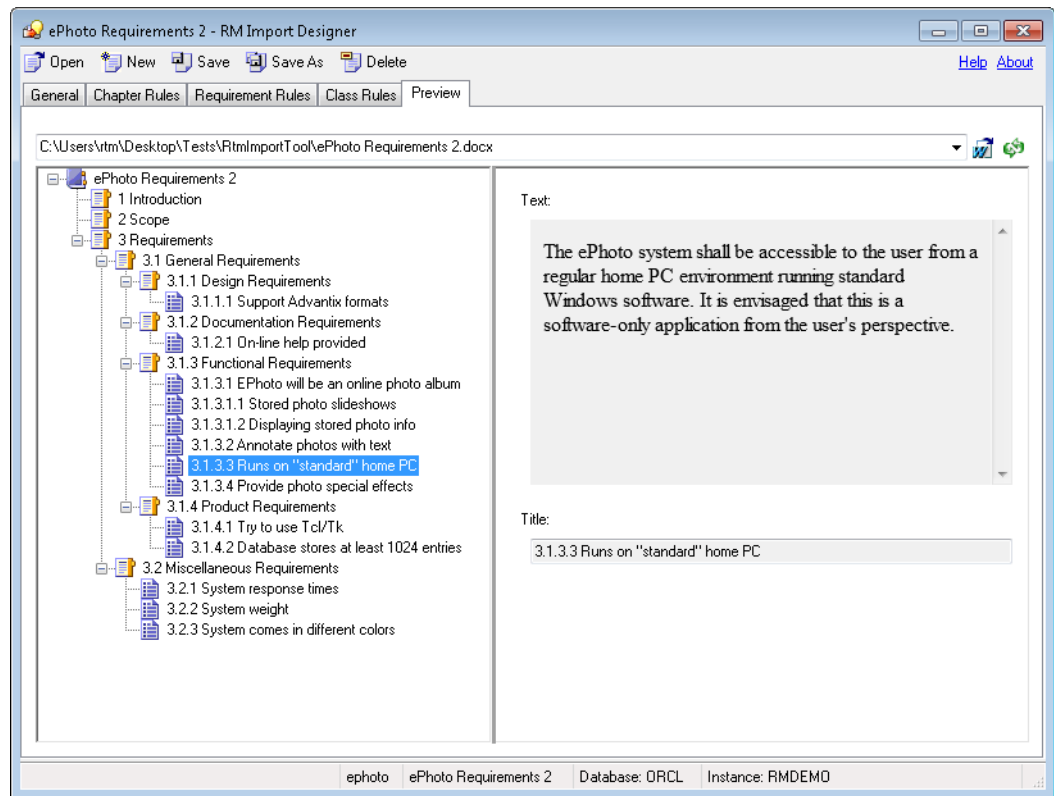
The next example shows what happens when you add a rule for the Title attribute.

## Capturing Title and Description with Title Rule

In this example, a wildcard character is specified in the **Attribute Rule** field, and the **Include keyword as part of requirement text** check box is selected. Using the **?** wildcard character means that the first sentence with any character will be captured as a title. Because there is a rule, the title will not be duplicated in the description.



A rule is specified, so there is no duplication between the **Text** and **Title** fields below.



**NOTE** For more information about wildcards, see ["Word Regular Expressions"](#) on page 425 and Microsoft Word documentation.



# URL Syntax

# How to Manually Specify a URL for URL Addressable Views

The *Dimensions RM Browser User's Guide* and the RM Browser Help show how to copy an object's URL from within RM Browser. However, if you wish to enter URLs by hand or use a script or program to invoke them, see the following for information on the correct syntax.



**NOTE** If an object name includes a space character, replace the space with: %20

## URL to a Document

```
http://ServerName/rtmBrowser/  
app?goto=doc&db=DataBaseName&proj=InstanceName&doc=DocumentName
```

## URL to a Chapter of a Document

```
http://ServerName/rtmBrowser/  
app?goto=doc&db=DataBaseName&proj=InstanceName&doc=DocumentName&class=Chapter&o=ChapterID
```

## URL to a Chapter, Requirement of a Document

```
http://ServerName/rtmBrowser/  
app?goto=doc&db=DataBaseName&proj=InstanceName&docID=19&c=1&pu id=MR  
KT_000040
```

## URL to a Snapshot of a Document

```
http://ServerName/rtmBrowser/  
?goto=doc&db=DataBaseName&proj=InstanceName&doc=SnapshotName
```

## URL to Export a Document

```
http://ServerName/rtmBrowser/cgi-bin/  
rtmBrowser.exe?&goto=publishdoc&db=DataBaseName&proj=InstanceName&docID  
=DocumentID&ic__saveAsOptions=doc
```

## URL to a Collection

```
http://ServerName/rtmBrowser/
?goto=collection&db=DataBaseName&proj=InstanceName&collection=CollectionName
```

After pasting the URL into a file or application, you can also add parameters to it, which allows additional features. If you do not supply run-time parameters in the URL, you can specify them when running the report.

Function	Description	Example URL
Editable Grid	By default, the requirements of collection or baseline are shown in a normal table. To use an editable grid instead, add <b>&amp;editableGrid=true</b> to the URL.	<code>http://myserver:8080/rtmBrowser/cgi-bin/rtmBrowser.exe?goto=collection&amp;db=ORCL&amp;proj=RMDEMO&amp;collection=CollectionName&amp;editableGrid=true</code>
Hide Title Bar	By default, the collection or baseline shows a title bar with information about database, instance and path to the report. To hide the title, add <b>&amp;hideTitleBar=true</b> to the URL.	<code>http://myserver:8080/rtmBrowser/cgi-bin/rtmBrowser.exe?goto=collection&amp;db=ORCL&amp;proj=RMDEMO&amp;collection=CollectionName&amp;hideTitleBar=true</code>

## URL to a Specific Version of a Requirement

```
http://ServerName/rtmBrowser/
?goto=req&db=DataBaseName&proj=InstanceName&class=ClassName&puid=Requirement'sPUID&ver=VersionNumber r
```



**NOTE** If no version is specified, it will default to 1.

## URL to compare History Versions of a Requirement

### Compare Requirement by Object Ids

```
http://ServerName/rtmBrowser/
?goto=req&db=DataBaseName&proj=InstanceName&class=ClassName&o=ObjectID1&comparewithID=ObjectID2
```

### Compare Current Requirement with Object Id

```
http://ServerName/rtmBrowser/
?goto=req&db=DataBaseName&proj=InstanceName&class=ClassName&puid=Requirement'sPUID&comparewithID=ObjectID
```

### Compare Requirement by Object Id and Version

```
http://ServerName/rtmBrowser/
?goto=req&db=DataBaseName&proj=InstanceName&class=ClassName&o=ObjectID&comparewith=Version
```

### Compare Two Versions of a Requirement

```
http://ServerName/rtmBrowser/
?goto=req&db=DataBaseName&proj=InstanceName&class=ClassName&puid=Requirement'sPUID&ver=Version1&comparewith=Version2
```

### Compare Current Requirement with a Version

```
http://ServerName/rtmBrowser/
?goto=req&db=DataBaseName&proj=InstanceName&class=ClassName&puid=Requirement'sPUID&comparewith=Version
```

### Specifying User Name and Password on an URL

For requirements, reports, collections, documents, snapshots, and to export documents, you can specify user name and password as part of the URL. This automatically logs you in and opens the requested item. Note that for login you also need to specify database name and instance name.

Option	Description	Example
u=	RM user name	u=epphoto
pwd=	RM password	pwd=rtm

## URL to the Current Version of a Requirement

```
http://ServerName/rtmBrowser/
?d=DataBaseName&p=InstanceName&f=2&c=ClassID&i=Requirement'sPUID&u=UserName&pwd=Password
```



**NOTE** This type of URL uses an older syntax that is different from the others. See the table below for more details on the options available in this syntax.

Option	Description	Example
d=	Oracle database that RM uses	d=RTM
pid=	RM instance ID number. You can specify pid= or p=, but not both (see "p=" below)	pid=2
p=	RM instance name. You can specify pid= or p=, but not both (see "pid=" above)	p=RMDEMO
f=	RM Action to perform. <ul style="list-style-type: none"><li>■ f=2: Opens an object for viewing.</li><li>■ f=4: Opens an edit dialog for the specified object.</li><li>■ f=5: Opens the RM browser home page.</li></ul>	f=2
c=	RM Class ID (this is a numeric value).	c=7
o=	RM Object ID (this is a numeric value).	o=21
u=	RM user name	u=epphoto
pwd=	RM password	pwd=rtm



# Appendix F

---

## Word Document Post Processing

Post Processing Overview	492
About Word Document Post Processor	492
About Custom Word Document Post Processor	499

---

## Post Processing Overview

Dimensions RM provides the function to process the Word document before it is made available for download. For this purpose, two command line tools can be executed: Word Document Post Processor and Custom Word Document Post Processor. By default, Word Document Post Processor is enabled by the setup program when installing the Dimensions RM server. The Word document export process is executed in this order:

- 1 Create an HTML document.
- 2 Create an MHTML document. This document also contains images and file attachments.
- 3 Run Word Document Post Processor, if configured.
- 4 Run Custom Word Document Post Processor, if configured.
- 5 Create a document in DOCX or PDF format, if a supported version of Microsoft Word has been installed on the server.

## About Word Document Post Processor

Word Document Post Processor is a command line tool, which processes the temporary HTML file created in the export process. It expects only the path to an HTML file as a command line parameter. The file name of Word Document Post Processor is WordDocumentPostProcessor.exe.

### Word Document Post Processor provides these functions:

- **Convert HTML lists (<ul> and <ol>) to Microsoft Word lists**  
Microsoft Word uses paragraphs (<p>) defined by class and style.
- **Remove unreferenced lists**  
Removes all list styles for which no list exists in the document.
- **Correct Empty Paragraphs**  
When exporting, empty paragraphs (<p></p>) may be present. These empty paragraphs are replaced by a style used by Word.
- **Correct image sizes**  
Images larger than the page width are resized. This function expects that the image is located in the main chapter. When images are within a table, it may be that the resized image are still too large, thus it is recommended to resize images accordingly when using them within a table.
- **Integrate sub-documents**  
When exporting requirements with a document, the requirements may have a full HTML document in HTML enabled text attributes. Word Document Post Processor merges these sub-documents and converts the encoding to match the main document.
- **Remove styles**  
Removes <style> tags from the body of the exported document.
- **Remove table size**  
Tables – especially tables with many columns – may exceed the page in the Word

document. Removing the table size allows Word to resize the columns. Most tables fit onto the page after removing the table size. However, if your table contains many long words, it may still exceed the page.

- **Remove WordSection1 or Section1**  
Usually, a Word document has only one <div> tag with class WordSection1 or Section1 defined. If more than one WordSection1 or Section1 is found, the class will be removed from that tag. This leaves the content intact, but defines it as a standard element.
- **Remove V:F Tags and parent V:\* Tags**  
V:F tags are used by Microsoft Word in combination with images. As Dimensions RM does not use V:F tags, these tags and surrounding tags (e.g. V:Formulas) can be removed to avoid any issues when opening the exported document.

#### **Word Document Post Processor provides these support functions:**

- **Backup of the input file**  
Word Document Post Processor creates a backup of the file which Word Document Post Processor will process. This file resides in the same directory as the original file. The file name contains the word "input" (e.g. wdp1913.input.tmp).
- **Backup of the output file**  
Word Document Post Processor creates a backup of the file which Word Document Post Processor processed. This file resides in the same directory as the original file. The file name contains the word "output" (e.g. wdp1913.output.tmp).
- **Logging**  
The log file WordDocumentPostProcessor.log resides in <RM Install Dir>\logs. Logging is configured in <RM Install Dir>\conf\log4net.config. For further information on configuration of logging, see chapter ["Log Files" on page 132](#).

## **Settings**

The following sections describe the settings which are configured through the WordDocumentPostProcessor.exe.config file, which resides in the <RM Install Dir>\bin folder. This config file is in XML format and must be edited with a text editor, e.g. Notepad.

Each setting is defined by the <setting> tag. Each setting is identified by its name attribute. A setting contains a <value> tag, which is used to configure the setting. The example below enables the **BackupInputFile** setting by setting it to **True**.

#### **Example:**

```
<setting name="BackupInputFile" serializeAs="String">
  <value>True</value>
</setting>
```

**List Settings**

Setting	Description
ConvertListsToWordLists	<p>If enabled, Word Document Post Processor converts HTML lists to Word lists.</p> <p><b>Possible values:</b></p> <ul style="list-style-type: none"> <li>■ False</li> <li>■ True</li> </ul> <p><b>Default: True</b> (turned on).</p>
List_Styles	<p>Contains styles which define the list layout. The IDs are required for Word Document Post Processor to recognize the lists. This setting should not be changed.</p>
List_Style_L1...9	<p>Defines the margin and indent for the list with the specified level. List_Style_L1 stands for lists with level 1, List_Style_L2 for lists with level 2, and so on.</p> <p><b>Default (for level 1): margin-left:72.0pt;mso-add-space:auto;text-indent:-18.0pt;</b></p>
RemoveStyles	<p>If enabled, Word Document Post Processor removes &lt;style&gt; tags within the body of the document.</p> <p><b>Possible values:</b></p> <ul style="list-style-type: none"> <li>■ False</li> <li>■ True</li> </ul> <p><b>Default: True</b> (turned on).</p>
RemoveUnreferencedLists	<p>If enabled, Word Document Post Processor removes styles for lists which are not present in the document.</p> <p><b>Possible values:</b></p> <ul style="list-style-type: none"> <li>■ False</li> <li>■ True</li> </ul> <p><b>Default: True</b> (turned on).</p>

Setting	Description
WordBulletListStyle_L1...9	<p>Defines the style for bullet lists. WordBulletListStyle_L1 stands for lists with level 1, WordBulletListStyle_L2 for lists with level 2, and so on. These list styles are only used for lists without a style definition in their UL tag.</p> <p><b>Possible values:</b></p> <ul style="list-style-type: none"> <li>▪ Bullet_Simple</li> <li>▪ Bullet_Empty</li> <li>▪ Bullet_Square</li> <li>▪ Bullet_Color</li> <li>▪ Bullet_Diamond</li> <li>▪ Bullet_Arrow</li> <li>▪ Bullet_Tick</li> </ul> <p><b>Defaults:</b>  <b>WordBulletListStyle_L1: Bullet_Simple</b>  <b>WordBulletListStyle_L2: Bullet_Empty</b>  <b>WordBulletListStyle_L3...9: Bullet_Square</b></p>
WordNumericListStyle_L1...9	<p>Defines the style for numeric lists. WordNumericListStyle_L1 stands for lists with level 1, WordNumericListStyle_L2 for lists with level 2, and so on. These list styles are only used for lists without a style definition in their OL tag.</p> <p><b>Possible values:</b></p> <ul style="list-style-type: none"> <li>▪ Number_Simple</li> <li>▪ Number_Parenthesis_Closing</li> <li>▪ Number_Parenthesis_Surrounding</li> <li>▪ Number_Abc_Lowercase</li> <li>▪ Number_Abc_Lowercase_Parenthesis_Closing</li> <li>▪ Number_Abc_Uppercase</li> <li>▪ Number_Abc_Uppercase_Parenthesis_Closing</li> <li>▪ Number_Roman_Capital</li> <li>▪ Number_Roman_Lowercase</li> <li>▪ Number_Greek_Lowercase</li> </ul> <p><b>Defaults:</b>  <b>WordNumericListStyle_L1: Number_Simple</b>  <b>WordNumericListStyle_L2: Number_Abc_Lowercase</b>  <b>WordNumericListStyle_L3...9: Number_Simple</b></p>

## Image Settings

Setting	Description
CorrectImageSize	<p>If enabled, Word Document Post Processor resizes images to fit the page.</p> <p><b>Possible values:</b></p> <ul style="list-style-type: none"> <li>■ False</li> <li>■ True</li> </ul> <p><b>Default: True</b> (turned on).</p>
ImgSubstractWidthInPixels	<p>Defines the number of pixels which to subtract from an image when resizing it.</p> <p><b>Possible values:</b></p> <ul style="list-style-type: none"> <li>■ Any integer (whole number) which is 0 or larger.</li> </ul> <p><b>Default: 10.</b></p>
MarginLeft	<p>Defines the width of the left margin. This setting is used for calculating the maximum image width. This setting accepts the following CSS formats: px, pt, in, mm, cm, and pc.</p> <p><b>Default: 1.25 in</b></p>
MarginRight	<p>Defines the width of the right margin. This setting is used for calculating the maximum image width. This setting accepts the following CSS formats: px, pt, in, mm, cm, and pc.</p> <p><b>Default: 1.25 in</b></p>
PageHeight	<p>Defines the height of the page. This settings is reserved for later use. This setting accepts the following CSS formats: px, pt, in, mm, cm, and pc.</p> <p><b>Default: 841.9 pt</b></p>
PageWidth	<p>Defines the width of the page. This setting is used for calculating the maximum image width. This setting accepts the following CSS formats: px, pt, in, mm, cm, and pc.</p> <p><b>Default: 595.3 pt</b></p>

**Other Settings**

Setting	Description
CorrectEmptyParagraphs	<p>If enabled, Word Document Post Processor corrects empty paragraphs.</p> <p><b>Possible values:</b></p> <ul style="list-style-type: none"> <li>■ False</li> <li>■ True</li> </ul> <p><b>Default: True</b> (turned on).</p>
IntegrateSubdocuments	<p>If enabled, Word Document Post Processor integrates sub-documents into the main document and converts the the encoding.</p> <p><b>Possible values:</b></p> <ul style="list-style-type: none"> <li>■ False</li> <li>■ True</li> </ul> <p><b>Default: True</b> (turned on).</p>
RemoveStyles	<p>If enabled, Word Document Post Processor removes &lt;style&gt; tags within the body of the document.</p> <p><b>Possible values:</b></p> <ul style="list-style-type: none"> <li>■ False</li> <li>■ True</li> </ul> <p><b>Default: True</b> (turned on).</p>
RemoveTableSize	<p>If enabled, Word Document Post Processor removes the width setting for tables.</p> <p><b>Possible values:</b></p> <ul style="list-style-type: none"> <li>■ False</li> <li>■ True</li> </ul> <p><b>Default: True</b> (turned on).</p>
RemoveUnwantedTags	<p>If enabled, Word Document Post Processor removes HTML undesired HTML tags.</p> <p><b>Possible values:</b></p> <ul style="list-style-type: none"> <li>■ False</li> <li>■ True</li> </ul> <p><b>Default: True</b> (turned on).</p>

Setting	Description
RemoveVfTags	<p>If enabled, Word Document Post Processor removes V:F tags and any parent tags in the "V" namespace.</p> <p><b>Possible values:</b></p> <ul style="list-style-type: none"> <li>■ False</li> <li>■ True</li> </ul> <p><b>Default: True</b> (turned on).</p>
RemoveWordSection1	<p>If enabled, Word Document Post Processor removes excess WordSection1 or Section1 class names.</p> <p><b>Possible values:</b></p> <ul style="list-style-type: none"> <li>■ False</li> <li>■ True</li> </ul> <p><b>Default: True</b> (turned on).</p>
BackupInputFile	<p>If enabled, Word Document Post Processor creates a backup of the file which Word Document Post Processor will process. This file resides in the same directory as the original file. The file name contains the word "input" (e.g. wdp1913.input.tmp).</p> <p><b>Possible values:</b></p> <ul style="list-style-type: none"> <li>■ False</li> <li>■ True</li> <li>■ <b>Default: False</b> (turned off).</li> </ul>
BackupOutputFile	<p>If enabled, Word Document Post Processor creates a backup of the file which Word Document Post Processor processed. This file resides in the same directory as the original file. The file name contains the word "output" (e.g. wdp1913.output.tmp).</p> <p><b>Possible values:</b></p> <ul style="list-style-type: none"> <li>■ False</li> <li>■ True</li> <li>■ <b>Default: False</b> (turned off).</li> </ul>

## Enabling Word Document Post Processor

To enable Word Document Post Processor, follow these steps:

- 1 Open Windows Registry editor (select **Run**, enter `regedit` and click **OK**).
- 2 Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft Focus\Dimensions RM\Environment\Default`
- 3 Right-click the **Default** key and select **New | DWORD (32-bit) Value** from the shortcut menu.
- 4 Name the new entry **WordDocumentPostProcessing\_Timeout** and press **Enter**.

- 5 Double-click **WordDocumentPostProcessing\_Timeout**.
- 6 Select option **Decimal** in the **Base** group.
- 7 Enter the number of seconds for the timeout into the **Value data** box. A good default is 600 (10 minutes).
- 8 Click **OK**.



#### NOTES

- The value of **WordDocumentPostProcessing\_Timeout** enables and disables Word document post processing. To disable Word document post processing, set the value to 0.
- The value of **WordDocumentPostProcessing\_Timeout** defines the maximum time WordDocumentPostProcessor.exe can use for correcting the document. If the timeout is exceeded, Dimensions RM will continue without using the corrected document. Note that this can result in a Document which cannot be opened by Microsoft Word.

## Disabling Word Document Post Processor

To disable Word Document Post Processor, follow these steps:

- 1 Open Windows Registry editor (select **Run**, enter `regedit` and click **OK**).
- 2 Navigate to  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft Focus\Dimensions RM\Environment\Default
- 3 Select the value **WordDocumentPostProcessing\_Timeout**.
- 4 Press the **Delete** (or **Del**) key on your keyboard. This opens the **Confirm Value Delete** dialog.
- 5 Click **Yes** to delete the value.

## About Custom Word Document Post Processor

Custom Word Document Post Processor allows to modify the Word document before it is presented to the user. As it is a custom tool, it is not part of Dimensions RM. Open Text Professional Services can create a Custom Word Document Post Processor for you that matches all of your requirements.

## Enabling Custom Word Document Post Processor

To enable Custom Word Document Post Processor, follow these steps:

- 1 Open Windows Registry editor (select **Run**, enter `regedit` and click **OK**).
- 2 Navigate to  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft Focus\Dimensions RM\Environment\Default

- 3 Right-click the **Default** key and select **New | DWORD (32-bit) Value** from the shortcut menu.
- 4 Name the new entry **CustomWordDocumentPostProcessing\_Timeout** and press **Enter**.
- 5 Double-click **CustomWordDocumentPostProcessing\_Timeout**.
- 6 Select option **Decimal** in the **Base** group.
- 7 Enter the number of seconds for the timeout into the **Value data** box. A good default is 600 (10 minutes).
- 8 Click **OK**.



#### NOTES

- The value of **CustomWordDocumentPostProcessing\_Timeout** enables and disables custom Word document post processing. To disable custom Word document post processing, set the value to 0.
- The value of **CustomWordDocumentPostProcessing\_Timeout** defines the maximum time CustomWordDocumentPostProcessor.exe can use for correcting the document. If the timeout is exceeded, Dimensions RM will continue without using the modified document.

## Disabling Custom Word Document Post Processor

**To disable Custom Word Document Post Processor, follow these steps:**

- 1 Open Windows Registry editor (select **Run**, enter regedit and click **OK**).
- 2 Navigate to  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Micro Focus\Dimensions RM\Environment\Default
- 3 Select the value **CustomWordDocumentPostProcessing\_Timeout**.
- 4 Press the **Delete** (or **Del**) key on your keyboard. This opens the **Confirm Value Delete** dialog.
- 5 Click **Yes** to delete the value.

## Appendix G

---

# Word Import Pre-Processing

Overview	502
Settings	502

---

## Overview

When importing Word documents or requirements from Word documents, the HTML code Microsoft® Word provides contains extra tags and styles. Word Import Pre-Processing is provided by the WordProcessing.dll file which is used by RM Browser and RM Import.

## Settings

The following sections describe the settings which are configured through the WordImportSettings.xml file, which resides in the <RM Install Dir>\conf folder. This configuration file is in XML format and must be edited with a text editor, e.g. Notepad.

Setting	Description
AllowEmptyListItems	<p>If enabled, Word Import Pre-Processing allows list items without content.</p> <p><b>Possible values:</b></p> <ul style="list-style-type: none"> <li>▪ false</li> <li>▪ true</li> </ul> <p><b>Default: false</b> (turned off).</p>
ConvertImages	<p>If enabled, Word Import Pre-Processing converts images in WMF or EMZ format to PNG.</p> <p><b>Possible values:</b></p> <ul style="list-style-type: none"> <li>▪ false</li> <li>▪ true</li> </ul> <p><b>Default: true</b> (turned on).</p>
ConvertWordListsToLists	<p>If enabled, Word Import Pre-Processing converts HTML lists to Word lists.</p> <p><b>Possible values:</b></p> <ul style="list-style-type: none"> <li>▪ false</li> <li>▪ true</li> </ul> <p><b>Default: true</b> (turned on).</p>
CorrectPNGImages	<p>If enabled, Word Import Pre-Processing checks if PNG images are faulty. If possible, a faulty PNG image is fixed.</p> <p><b>Possible values:</b></p> <ul style="list-style-type: none"> <li>▪ false</li> <li>▪ true</li> </ul> <p><b>Default: true</b> (turned on).</p>

Setting	Description
RemoveComments	<p>If enabled, Word Import Pre-Processing removes all comments.</p> <p><b>Possible values:</b></p> <ul style="list-style-type: none"> <li>■ false</li> <li>■ true</li> </ul> <p><b>Default: true</b> (turned on).</p>
RemoveIfEndif	<p>If enabled, Word Import Pre-Processing removes all [if ...] and [endif] tags.</p> <p><b>Possible values:</b></p> <ul style="list-style-type: none"> <li>■ false</li> <li>■ true</li> </ul> <p><b>Default: true</b> (turned on).</p>
RemoveOfficeParagraphs	<p>If enabled, Word Import Pre-Processing removes all O:P tags, preserving the content.</p> <p><b>Possible values:</b></p> <ul style="list-style-type: none"> <li>■ false</li> <li>■ true</li> </ul> <p><b>Default: true</b> (turned on).</p>
RemoveTableSize	<p>If enabled, Word Import Pre-Processing removes the width setting for tables</p> <p><b>Possible values:</b></p> <ul style="list-style-type: none"> <li>■ false</li> <li>■ true</li> </ul> <p><b>Default: true</b> (turned on).</p>
RemoveVfTags	<p>If enabled, Word Import Pre-Processing removes V:F tags and any parent tags in the "V" namespace.</p> <p><b>Possible values:</b></p> <ul style="list-style-type: none"> <li>■ False</li> <li>■ True</li> </ul> <p><b>Default: True</b> (turned on).</p>
RemoveWordSections	<p>If enabled, Word Import Pre-Processing removes any class name starting with WordSection or Section.</p> <p><b>Possible values:</b></p> <ul style="list-style-type: none"> <li>■ false</li> <li>■ true</li> </ul> <p><b>Default: true</b> (turned on).</p>

Setting	Description
ReplaceClassesWithStyles	<p>If enabled, Word Import Pre-Processing replaces classes for HTML tags in the Word document with styles. This setting corresponds with the <b>ReplaceClassWithStyles</b> setting in chapter "<a href="#">Selector Settings</a>" on page 506.</p> <p><b>Possible values:</b></p> <ul style="list-style-type: none"><li>■ false</li><li>■ true</li></ul> <p><b>Default: true</b> (turned on).</p>
ReplaceImages	<p>If enabled, Word Import Pre-Processing replaces low-resolution images with their high-resolution counterparts if available.</p> <p><b>Possible values:</b></p> <ul style="list-style-type: none"><li>■ false</li><li>■ true</li></ul> <p><b>Default: true</b> (turned on).</p>

Setting	Description
WordBulletListStyle_L1...9	<p>Defines the style for bullet lists. WordBulletListStyle_L1 stands for lists with level 1, WordBulletListStyle_L2 for lists with level 2, and so on. These list styles are only used for lists without a style definition in their UL tag.</p> <p><b>Possible values:</b></p> <ul style="list-style-type: none"> <li>■ Bullet_Simple</li> <li>■ Bullet_Empty</li> <li>■ Bullet_Square</li> <li>■ Bullet_Color</li> <li>■ Bullet_Diamond</li> <li>■ Bullet_Arrow</li> <li>■ Bullet_Tick</li> </ul> <p><b>Defaults:</b>  <b>WordBulletListStyle_L1: Bullet_Simple</b>  <b>WordBulletListStyle_L2: Bullet_Empty</b>  <b>WordBulletListStyle_L3...9: Bullet_Square</b></p>
WordNumericListStyle_L1...9	<p>Defines the style for numeric lists. WordNumericListStyle_L1 stands for lists with level 1, WordNumericListStyle_L2 for lists with level 2, and so on. These list styles are only used for lists without a style definition in their OL tag.</p> <p><b>Possible values:</b></p> <ul style="list-style-type: none"> <li>■ Number_Simple</li> <li>■ Number_Parenthesis_Closing</li> <li>■ Number_Parenthesis_Surrounding</li> <li>■ Number_Abc_Lowercase</li> <li>■ Number_Abc_Lowercase_Parenthesis_Closing</li> <li>■ Number_Abc_Uppercase</li> <li>■ Number_Abc_Uppercase_Parenthesis_Closing</li> <li>■ Number_Roman_Capital</li> <li>■ Number_Roman_Lowercase</li> <li>■ Number_Greek_Lowercase</li> </ul> <p><b>Defaults:</b>  <b>WordNumericListStyle_L1: Number_Simple</b>  <b>WordNumericListStyle_L2: Number_Abc_Lowercase</b>  <b>WordNumericListStyle_L3...9: Number_Simple</b></p>

Setting	Description
CorrectImageSize	If enabled, Word Import Pre-Processing resizes images to fit the page. <b>Possible values:</b> <ul style="list-style-type: none"><li>False</li><li>True</li></ul> <b>Default: True</b> (turned on).

## Selector Settings

Selector settings are used to remove attributes, classes, styles, or tags or to replace classes with styles. For comparing names and values, the following settings can be used:

- Contains
- Equals
- StartsWith

Tag names, attribute names and style names are compared case insensitive. To compare values case sensitive, set the related IgnoreCase setting (e.g. AttributeValueIgnoreCase) to true. To compare case insensitive, set the setting to false.

Setting	Description
RemoveAttributes	<p>If configured, Word Import Pre-Processing removes all attributes that match the selectors.</p> <p><b>Default:</b></p> <pre>&lt;RemoveAttributes&gt;   &lt;Attribute&gt;     &lt;!--Removes all attributes with a     namespace.--&gt;     &lt;AttributeName&gt;:&lt;/AttributeName&gt;     &lt;AttributeNameComparison&gt;Contains&lt;/     AttributeNameComparison&gt;     &lt;AttributeValue /&gt;     &lt;AttributeValueComparison&gt;Equals&lt;/     AttributeValueComparison&gt;     &lt;AttributeValueIgnoreCase&gt;&gt;false&lt;/     AttributeValueIgnoreCase&gt;   &lt;/Attribute&gt; &lt;/RemoveAttributes&gt;</pre>
RemoveClasses	<p>If configured, Word Import Pre-Processing removes all classes (entries from the class attribute) that match the selectors.</p> <p><b>Default:</b></p> <pre>&lt;RemoveClasses&gt;   &lt;Class&gt;     &lt;!--Removes all Office Mso classes.--&gt;     &lt;ClassName&gt;mso&lt;/ClassName&gt;     &lt;ClassNameComparison&gt;StartsWith&lt;/     ClassNameComparison&gt;     &lt;ClassNameIgnoreCase&gt;&gt;true&lt;/     ClassNameIgnoreCase&gt;   &lt;/Class&gt; &lt;/RemoveClasses&gt;</pre>
RemoveStyles	<p>If configured, Word Import Pre-Processing removes all styles (entries from the style attribute) that match the selectors.</p> <p><b>Default:</b></p> <pre>&lt;RemoveStyles&gt;   &lt;Style&gt;     &lt;!--Removes all Office Mso styles.--&gt;     &lt;StyleName&gt;mso&lt;/StyleName&gt;     &lt;StyleNameComparison&gt;StartsWith&lt;/     StyleNameComparison&gt;     &lt;StyleValue /&gt;     &lt;StyleValueComparison&gt;Equals&lt;/     StyleValueComparison&gt;     &lt;StyleValueIgnoreCase&gt;&gt;false&lt;/     StyleValueIgnoreCase&gt;   &lt;/Style&gt; &lt;/RemoveStyles&gt;</pre>

Setting	Description
RemoveTags	<p>If configured, Word Import Pre-Processing removes all tags that match the selectors.</p> <p><b>Default:</b></p> <pre> &lt;RemoveTags&gt;   &lt;Tag&gt;     &lt;!--Removes all Office style tags--&gt;     &lt;TagName&gt;style&lt;/TagName&gt;     &lt;TagNameComparison&gt;Equals&lt;/ TagNameComparison&gt;     &lt;Attributes /&gt;     &lt;AttributeSelectionMode&gt;Any&lt;/ AttributeSelectionMode&gt;     &lt;Classes /&gt;     &lt;ClassesSelectionMode&gt;Any&lt;/ ClassesSelectionMode&gt;     &lt;Styles /&gt;     &lt;StylesSelectionMode&gt;Any&lt;/ StylesSelectionMode&gt;     &lt;PreserveChildren&gt;true&lt;/ PreserveChildren&gt;     &lt;RemoveOnlyIfEmpty&gt;&gt;false&lt;/ RemoveOnlyIfEmpty&gt;   &lt;/Tag&gt;   &lt;Tag&gt;     &lt;!--Removes all tags with a namespace and preserves the child nodes.--&gt;     &lt;TagName&gt;:&lt;/TagName&gt;     &lt;TagNameComparison&gt;Contains&lt;/ TagNameComparison&gt;     &lt;Attributes /&gt;     &lt;AttributeSelectionMode&gt;Any&lt;/ AttributeSelectionMode&gt;     &lt;Classes /&gt;     &lt;ClassesSelectionMode&gt;Any&lt;/ ClassesSelectionMode&gt;     &lt;Styles /&gt;     &lt;StylesSelectionMode&gt;Any&lt;/ StylesSelectionMode&gt;     &lt;PreserveChildren&gt;true&lt;/ PreserveChildren&gt;     &lt;RemoveOnlyIfEmpty&gt;&gt;false&lt;/ RemoveOnlyIfEmpty&gt;   &lt;/Tag&gt; &lt;/RemoveTags&gt; </pre>

Setting	Description
ReplaceClassWithStyles	<p>If configured, Word Import Pre-Processing sets styles for the specified all class (entry from the class attribute).</p> <p>The <b>Mode</b> setting can have these values:</p> <ul style="list-style-type: none"> <li>■ Ignore</li> <li>■ RemoveClassOnly</li> <li>■ AddDocumentStyleOnly</li> <li>■ AddDocumentStyleAndRemoveClass</li> <li>■ AddSpecifiedStyleOnly</li> <li>■ AddSpecifiedStyleAndRemoveClass</li> <li>■ AddDocumentStyleOrSpecifiedStyleOnly</li> <li>■ AddDocumentStyleOrSpecifiedStyleOnlyAndRemoveClass</li> </ul> <p><b>Default:</b></p> <pre>&lt;ReplaceClassWithStyles&gt;   &lt;ReplaceClassWithStyle&gt;     &lt;TagName /&gt;     &lt;TagNameComparison&gt;Equals&lt;/ TagNameComparison&gt;     &lt;ClassName&gt;msolistparagraph&lt;/ ClassName&gt;     &lt;ClassNameComparison&gt;StartsWith&lt;/ ClassNameComparison&gt;     &lt;ClassNameIgnoreCase&gt;&gt;true&lt;/ ClassNameIgnoreCase&gt;     &lt;Mode&gt;AddDocumentStyleOnly&lt;/Mode&gt;     &lt;StyleValue /&gt;   &lt;/ReplaceClassWithStyle&gt;   &lt;ReplaceClassWithStyle&gt;     &lt;TagName /&gt;     &lt;TagNameComparison&gt;Equals&lt;/ TagNameComparison&gt;     &lt;ClassName&gt;*&lt;/ClassName&gt;     &lt;ClassNameComparison&gt;Equals&lt;/ ClassNameComparison&gt;     &lt;ClassNameIgnoreCase&gt;&gt;false&lt;/ ClassNameIgnoreCase&gt;     &lt;Mode&gt;AddDocumentStyleOnly&lt;/Mode&gt;     &lt;StyleValue&gt;&lt;/StyleValue&gt;   &lt;/ReplaceClassWithStyle&gt; &lt;/ReplaceClassWithStyles&gt;</pre>



## Appendix H

---

# Automatic Termination of MS Word

Overview	512
Settings	512

---

## Overview

When importing Word documents or requirements from Word documents, or exporting Dimensions RM documents or requirements to Word or PDF format, it may occur that Microsoft® Word may be unable to perform the desired function in the expected time. To avoid that the memory used during the process is never freed, ForceExit.exe will terminate the specific Microsoft® Word process after the configured time.

## Settings

The following sections describe the settings which are configured through the ForceExit.exe.config file, which resides in the <RM Install Dir>\bin folder. This config file is in XML format and must be edited with a text editor, e.g. Notepad.

Each setting is defined by the <setting> tag. Each setting is identified by its name attribute. A setting contains a <value> tag, which is used to configure the setting. The example below sets the polling interval to 5 minutes.

**Example:**

```
<setting name="PollingIntervalInMinutes" serializeAs="String">
  <value>5</value>
</setting>
```

Setting	Description
MaximumRunTimeInMinutes	Specifies the maximum time in minutes the target process may run.  <b>Possible values:</b> Any integer greater than 9. <b>Default: 60</b>
PollingIntervalInMinutes	Specifies the time ForceExit checks if the target process has terminated  <b>Possible values:</b> Any integer greater than 0. <b>Default: 5</b>

## Appendix I

---

# Configuration and Usage of ServiceHelper

Overview	514
Settings	514
Usage	518

---

## Overview

ServiceHelper is a command-line tool to support functionality with Dimensions RM, e.g. for managing Dimensions RM related services.

## Settings

The following table describes the settings which are configured through the ServiceHelper.exe.config file, which resides in the <RM Install Dir>\bin folder. This config file is in XML format and must be edited with a text editor, e.g. Notepad.

Each setting is defined by the <setting> tag and is identified by its name attribute. A setting contains a <value> tag, which is used to configure the setting. The example below disables the functionality to restart Tomcat.

**Example:**

```
<setting name="MANAGE_COMMON_TOMCAT" serializeAs="String">
  <value>False</value>
</setting>
```

Setting	Description
MANAGE_COMMON_TOMCAT	Specifies ability to restart Tomcat.  <b>Possible values:</b> True, False <b>Default: True</b>
RESTART_TOMCAT_ATTEMPTS	Specifies the maximum number of attempts to restart Tomcat.  <b>Possible values:</b> 2 or larger integer value <b>Default: 5</b>
RESTART_TOMCAT_ATTEMPTS_WAIT_SECONDS	Specifies the time in seconds to wait between Tomcat restart attempts.  <b>Possible values:</b> 30 or larger integer value <b>Default: 30</b>
RESTART_TOMCAT_WAIT_SECONDS	Specifies the time in seconds to allow Tomcat to restart.  <b>Possible values:</b> 30 or larger integer value <b>Default: 120</b>

Setting	Description
SECURITY_PROTOCOL	<p>Specifies the security protocol(s) to use when verifying that Tomcat has restarted successfully. These values must contain the same.</p> <p><b>Possible values:</b> Depends on installed .NET framework version:</p> <ul style="list-style-type: none"> <li>.NET 4.0: SSL3 TLS</li> <li>.NET 4.5: SSL3 TLS TLS11 TLS12</li> <li>.NET 4.8: SSL3 TLS TLS11 TLS12 TLS13</li> </ul> <p><b>Default: SSL3 TLS</b></p>
SERVICE_NAME_POOL_MANAGER	<p>Specifies the name of the RM Pool Manager service. Do not modify this value.</p> <p><b>Possible values:</b> RMPoolManager <b>Default: RMPoolManager</b></p>
SERVICE_NAME_TOMCAT	<p>Specifies the name of the Tomcat service. Change this only if you do not use Open Text Common Tomcat.</p> <p><b>Possible values:</b> Any string with at least one character <b>Default: opentextTomcat</b></p>
START_SERVICE_WAIT_SECONDS	<p>Specifies the time in seconds to allow a service to start.</p> <p><b>Possible values:</b> 5 or larger integer value <b>Default: 40</b></p>
START_STOP_SERVICE_ATTEMPTS	<p>Specifies the number of attempts to start or stop a service.</p> <p><b>Possible values:</b> 1 or larger integer value <b>Default: 5</b></p>
START_STOP_STOP_SERVICE_ATTEMPTS_WAIT_SECONDS	<p>Specifies the time in seconds to wait between start or stop attempts.</p> <p><b>Possible values:</b> 5 or larger integer value <b>Default: 40</b></p>
STOP_SERVICE_WAIT_SECONDS	<p>Specifies the time in seconds to allow a service to stop.</p> <p><b>Possible values:</b> 5 or larger integer value <b>Default: 25</b></p>

Setting	Description
SYSTEMINFO_COMMON_TOOLS_SHOW_PATH	<p>Specifies if the path to Dimensions RM Common Tools should be included with the system information file.</p> <p><b>Possible values:</b> True, False <b>Default:</b> True</p>
SYSTEMINFO_COMMON_TOOLS_SHOW_VERSION	<p>Specifies if the Dimensions RM Common Tools version should be included with the system information file.</p> <p><b>Possible values:</b> True, False <b>Default:</b> True</p>
SYSTEMINFO_DATABASE_SHOW_NAME	<p>Specifies if the database name (e.g. Oracle) should be included with the system information file.</p> <p><b>Possible values:</b> True, False <b>Default:</b> True</p>
SYSTEMINFO_DATABASE_SHOW_ODBC_VERSION	<p>Specifies if the version of the ODBC driver should be included with the system information file.</p> <p><b>Possible values:</b> True, False <b>Default:</b> True</p>
SYSTEMINFO_DATABASE_SHOW_VERSION	<p>Specifies if the database version should be included with the system information file.</p> <p><b>Possible values:</b> True, False <b>Default:</b> True</p>
SYSTEMINFO_MSOFFICE_SHOW_PATH	<p>Specifies if the path to Microsoft Office should be included with the system information file.</p> <p><b>Possible values:</b> True, False <b>Default:</b> True</p>
SYSTEMINFO_MSOFFICE_SHOW_VERSION	<p>Specifies if the version of the Microsoft Office should be included with the system information file.</p> <p><b>Possible values:</b> True, False <b>Default:</b> True</p>
SYSTEMINFO_OS_SHOW_DOTNET	<p>Specifies if the installed .NET frameworks should be included with the system information file.</p> <p><b>Possible values:</b> True, False <b>Default:</b> True</p>

Setting	Description
SYSTEMINFO_OS_SHOW_DRIVES	<p>Specifies the drives than can be included with the system information file. To include all drives, use *. Alternatively specify the drive letters separated by semicolon (e.g. C;D)</p> <p><b>Possible values:</b> * or valid drive letters <b>Default:</b> *</p>
SYSTEMINFO_OS_SHOW_ENVIRONMENT_VARIABLES	<p>Specifies if the environment variables should be included with the system information file.</p> <p><b>Possible values:</b> True, False <b>Default:</b> True</p>
SYSTEMINFO_OS_SHOW_RAM	<p>Specifies if free RAM and total RAM should be included with the system information file.</p> <p><b>Possible values:</b> True, False <b>Default:</b> True</p>
SYSTEMINFO_OS_SHOW_VERSION	<p>Specifies if the version of the operating system should be included with the system information file.</p> <p><b>Possible values:</b> True, False <b>Default:</b> True</p>
SYSTEMINFO_RM_SHOW_PATH	<p>Specifies if the path to Dimensions RM should be included with the system information file.</p> <p><b>Possible values:</b> True, False <b>Default:</b> True</p>
SYSTEMINFO_WEBSERVER_SHOW_NAME	<p>Specifies if the name of the web server (usually Tomcat) should be included with the system information file.</p> <p><b>Possible values:</b> True, False <b>Default:</b> True</p>
SYSTEMINFO_WEBSERVER_SHOW_PATH	<p>Specifies if the path to the web server (usually Open Text Common Tomcat) should be included with the system information file.</p> <p><b>Possible values:</b> True, False <b>Default:</b> True</p>

Setting	Description
SYSTEMINFO_WEBSERVER_SHOW_VERSION	<p>Specifies if the web server version should be included with the system information file.</p> <p><b>Possible values:</b> True, False <b>Default: True</b></p>
VALIDATION_URL_FORMAT	<p>Specifies the format of the URL to verify that Tomcat has restarted successfully. Do not modify this value.</p> <p><b>Possible values:</b> {0}:{1}/rtmBrowser/cgi-bin/rtmBrowser.exe <b>Default: {0}:{1}/rtmBrowser/cgi-bin/rtmBrowser.exe</b></p>

## Usage

### Retrieving Dimensions RM Configuration

This function retrieves the configuration (Windows registry, and status of RM related services) and stores it as an XML file.

Parameter	Description
Action	GetRMConfiguration
OutputFile	Specify the path to the file to receive the RM configuration in XML format.

**Example** (all on one line):

```
ServiceHelper.exe /Action GetRMConfiguration
/OutputFile C:\temp\RMConfig.xml
```

### Getting a List of RM Services

This function retrieves a list of RM related services including there status and stores it as an XML file. This list is also part of ["Retrieving Dimensions RM Configuration" on page 518](#).

Parameter	Description
Action	GetServiceList
OutputFile	Specify the path to the file to receive the service list in XML format.

**Example** (all on one line):

```
ServiceHelper.exe /Action GetServiceList
/OutputFile C:\temp\services.xml
```

## Getting System Information

This function retrieves system information as allowed by configuration (see chapter "Settings" on page 514). Note that the database information is specified by command-line options.

Parameter	Description
Action	GetSystemInformation
OutputFile	Specify the path to the file to receive the RM configuration in XML format.
Database	Specify the database connection to appear in the XML file.
DatabaseName	Specify the database name (e.g. Oracle) to appear in the XML file.
DatabaseVersion	Specify the database version to appear in the XML file.

**Example** (all on one line):

```
ServiceHelper.exe /Action GetSystemInformation
/OutputFile C:\temp\systeminformation.xml
/Database RM
/DatabaseName Oracle
/DatabaseVersion 19.0
```

## Importing Certificates into a System Keystore

This function imports certificates into the Windows keystore.

Parameter	Description
Action	ImportSystemCertificate
SystemCertStore	Any value as specified in .NET StoreName enumeration (in System.Security.Cryptography.X509Certificates). Recommended values: <ul style="list-style-type: none"> <li>▪ <b>Root:</b> Import into Trusted Root Certificate Authorities keystore</li> <li>▪ <b>CertificateAuthority:</b> Import into Intermediate Certificate Authorities keystore</li> </ul>
InputCert	The full path to the certificate to import.

**Examples** (all on one line):

```
ServiceHelper.exe /Action ImportSystemCertificate
/SystemCerteStore Root
/InputCert C:\temp\rootCA.cer
```

```
ServiceHelper.exe /Action ImportSystemCertificate
/SystemCerteStore CertificateAuthority
/InputCert C:\temp\intermediateCA0.cer
```

## Restarting RM Pool Manager

This function restarts the RM Pool manager.

Parameter	Description
Action	RestartPoolManager
OutputFile	Specify the path to the file to receive the restart result as plain text.

**Example** (all on one line):

```
ServiceHelper.exe /Action RestartPoolManager
/OutputFile C:\temp\restartresult.txt
```

## Restarting Tomcat

This function restarts the Tomcat service (usually Open Text Common Tomcat).

Parameter	Description
Action	RestartTomcatSimple
OutputFile	Specify the path to the file to receive the restart result as plain text.
ValidationUrl	<p>Specify the validation URL in this format: <i>protocol://server:port/rtmBrowser</i></p> <p>Replace the format values like this:</p> <ul style="list-style-type: none"> <li>▪ <b>protocol:</b> must be http or https</li> <li>▪ <b>server:</b> The name of the machine. For HTTP, it can be localhost. For HTTPS the name must match the name of the certificate.</li> <li>▪ <b>port:</b> The port to use. If you do not need a port when accessing Dimensions RM in the web browser, use these default ports: <ul style="list-style-type: none"> <li>• <b>For HTTP:</b> 80</li> <li>• <b>For HTTPS:</b> 443</li> </ul> </li> </ul>

**Example** (all on one line):

```
ServiceHelper.exe /Action RestartTomcatSimple
/OutputFile C:\temp\restartresult.txt
/ValidationUrl http://localhost:8080/rtmBrowser
```

## Restarting a Service

This function restarts the specified service.

Parameter	Description
Action	RestartService
Service	Specify the service name.
OutputFile	Specify the path to the file to receive the restart result as plain text.

**Example** (all on one line):

```
ServiceHelper.exe /Action RestartService
/Service SERVICE_NAME
/OutputFile C:\temp\restartresult.txt
```

## Starting a Service

This function starts the specified service.

Parameter	Description
Action	StartService
Service	Specify the service name.
OutputFile	Specify the path to the file to receive the start result as plain text.

**Example** (all on one line):

```
ServiceHelper.exe /Action StartService
/Service SERVICE_NAME
/OutputFile C:\temp\startresult.txt
```

## Stopping a Service

This function stops the specified service.

Parameter	Description
Action	StopService

Parameter	Description
Service	Specify the service name.
OutputFile	Specify the path to the file to receive the stop result as plain text.

**Example** (all on one line):

```
ServiceHelper.exe /Action StopService
/Service SERVICE_NAME
/OutputFile C:\temp\stopresult.txt
```

## Splitting a PFX Certificate

This function splits the PFX certificate chain into separate files. The files will reside in the same directory as the original certificate. file names are:

- **ca0.cer:** The certificate of the root certification authority.
- **ca#.cer:** Starting with ca1.cer; the certificates of the intermediate authorities
- **server.cer:** The certificate of the server to be certified.

Parameter	Description
Action	SplitCertificate
InputCert	Specify the path to the certificate in PFX format.
InputCertPwd	Specify the certificate password.

**Example** (all on one line):

```
ServiceHelper.exe /Action SplitCertificate
/InputCert C:\Certificates\cert1.pfx
/InputCertPwd myPassword
```

# Appendix J

---

## Azure Active Directory

Registering Dimensions RM as Azure Application	524
Retrieving Configuration Data from Azure AD	525
Azure SAML2 Authentication	528

# Microsoft Azure

## Registering Dimensions RM as Azure Application

Dimensions RM can use Microsoft Azure as a login source. As such, passwords for users with user type **LDAP or SSO** are authenticated against Microsoft Azure. Before you begin, ensure that you have the login for the administrative account.



**NOTE** The Azure AD authentication that was used in earlier releases with OAuth protocol must be reconfigured to use the new settings see section

To register Dimensions RM as an Azure application:

- 1 Open the Azure portal in your web browser (<https://portal.azure.com>).
- 2 Log in with your administrative account, e.g. `admin@usernamedomain.onmicrosoft.com`.
- 3 Select **Azure Active Directory**.
- 4 Select **App registrations**.
- 5 Select **New registration**.
- 6 Enter a name into the **Name** box to identify your Dimensions RM application.
- 7 Select the **Accounts in the organizational directory only** option.
- 8 Specify the Redirect URI
  - a Ensure that Web is selected.
  - b Specify the URL for Dimensions RM, e.g. `https://myserver.mydomain:8443/rtmBrowser/`  
Replace *myserver*, *mydomain* and *8443* with server name, domain and port of your Dimensions RM installation.
- 9 Click **Register**. This creates the Azure app entry with the name you specified.
- 10 Select **Certificates & secrets**.
- 11 Click **New client secret**. This opens the **Add a client secret** dialog.
- 12 Select the desired expiry time.
- 13 Click **Add**.



**IMPORTANT!** Copy the secret value and save it as a file.

- 14 Select **API permissions**.
- 15 Click **Add a permission**. This opens the **Request API permissions** dialog.
- 16 Select **Microsoft Graph**.

- 17 Select **Delegated permissions**.
- 18 Select **Directory.AccessAsuser.All**.
- 19 Select **User.Read**.
- 20 Click **Add permissions**.
- 21 Select **Authentication**.
- 22 Click **Add URI**.
- 23 Enter the following URI: `https://myserver.mydomain:8443/rtmBrowser/auth`  
Replace *myserver*, *mydomain* and *8443* with server name, domain and port of your Dimensions RM installation i.e. `https://ormtestit-rm05:8443/rtmBrowser/auth`  

Note that this URI is very similar to the one entered in step 8b. Here however, the trailing slash has been removed. It is important to specify this URI as well as users may have to specify the trailing slash otherwise.
- 24 Select option **ID tokens**.
- 25 Click **Save**.

## Retrieving Configuration Data from Azure AD

Before retrieving the configuration data from Azure, ensure that you registered Dimensions RM as Azure application. For details, see, "[Registering Dimensions RM as Azure Application](#)" on page 524

It is simpler to gather the data before updating the configuration, we recommend opening a file with, for example, notepad to save the settings. You will need **Tenant**, **client\_uri**, **client\_id**, **Client\_secret\_key**.

### To retrieve the configuration data from Azure AD:

- 1 Open the Azure portal in your web browser (<https://portal.azure.com>).
- 2 Log in with your administrative account, e.g. `admin@usernamedomain.onmicrosoft.com`.
- 3 **To retrieve the Tenant, do the following:**
  - a Select **Azure Active Directory**.
  - b Select **Custom domain names**.
  - c From the list, take the **Name** value with this format: `usernamedomain.onmicrosoft.com` as the tenant.
  - d **Copy the tenant ID, by executing the following steps:**
    - A Click the icon next to the tenant ID to copy the ID into the Windows Clipboard.
    - B Open Notepad.
    - C In Notepad, copy **Ctrl+V**.
- 4 **To retrieve the Client ID and Client ID URI, do the following:**

- a Select **Azure Active Directory**.
  - b Select **App registrations**.
  - c Select the desired app.
  - d Select **Overview**.
  - e Copy the value from the **App ID URI**. This is the **Client ID URI**.
  - f Copy the value from the **Application (client) ID**. This is the **Client ID**.
- 5 To retrieve the Issuer URL, do the following:**
  - a Copy **tenantID** and place into the Issuer URL. For example  
`https://login.microsoftonline.com/<tenantID>/v2.0`
- 6 To retrieve the Trust Certificate, do the following:**
  - a Navigate to the following URL: [https://login.microsoftonline.com/{tenant\\_id}/discovery/keys](https://login.microsoftonline.com/{tenant_id}/discovery/keys).  
Replace **{tenant\_id}** with the ID you retrieved in [Step 3](#).
  - b Open Notepad, with a new file.
  - c Type **default:** (including the colon).
  - d From the Active Directory page, copy the certificate from the entry with key 0 to the clipboard by pressing **Ctrl+C**.
  - e Switch back to Notepad. Type a blank and paste the value from the clipboard by pressing **Ctrl+V**.  
**Example:**  
default: MIIDB...
  - f For any other certificate from the Active Directory page, execute the following steps:
    - A** In Notepad, create a new line.
    - B** From the Active Directory page, copy the key ID to the clipboard by pressing **Ctrl+C**.
    - C** Switch back to Notepad. Paste the value for `kid` from the clipboard by pressing **Ctrl+V**.
    - D** From the Active Directory page, copy the certificate entry (`x5c -> 0`) to the clipboard by pressing **Ctrl+C**.
    - E** Switch back to Notepad. Type colon and a blank and press **Ctrl+V**.  
**Example:**  
VGhpcyBpcyBhIFNhbXBsZSBvbmx5: MIIDB...
  - g Save the file with file extension **pem** (e.g. sts.pem).
- 7 The JWKS (JSON Web Key Set) URI (Optional)**

The JWKS URI can be included in order to automatically update public certificates in sts.pem when they are changed through a periodic update by Azure.

The format is `https://login.microsoftonline.com/{tenantID}/discovery/v2.0/keys` with **{tenantID}** replaced with the value retrieved in [Step 3](#).

- 8 Copy *RM\_Install*\Common Tools *###.#*\tomcat\*##*\webapps\rtmBrowser\WEB-INF\web.xml to a backup - just to be safe.
- 9 Open *RM\_Install*\Common Tools *###.#*\tomcat\*##*\webapps\rtmBrowser\WEB-INF\web.xml with a text editor, e.g. Notepad.
- 10 Search for **Azure SSO Filter**
- 11 Modify as follows:
  - a Uncomment the filter section.
  - b Set filter-name, param-value to **true**
  - c Set **Tenant** param-value to tenant, as saved above.
  - d Set **client\_uri** param-value to **client\_uri**, as saved above.
  - e Set **client\_id** param-value to **client\_id**, as saved above.
  - f Set **client\_secret\_key** param-value to **client\_secret\_key**, as saved above.
  - g Save web.xml
- 12 Configure login sources, checking **RM** and **Azure AD** (see "[Configuring E-Mail Notification](#)" on page 240). Enable Auto Create and add new user to default Instance and Group.
- 13 Click Settings for Azure AD (all must be populated):
  - a **Authority**: e.g. https://login.windows.net/
  - b **Tenant**: as saved
  - c **Client ID URI**: as saved
  - d **Client ID**: as saved
  - e Security Token Service (STS) **Issuer URL**: Federation Server URL should look something like: https://login.microsoftonline.com/00000000-0000-0000-0000-000000000000
  - f Security Token Service (STS) **Trust Certificate**: enter path to rm\conf\sts.pem
  - g JWKS (JSON Web Key Set) URI if applied.

**Figure J-1. Configure Login Settings, Azure AD, Settings**

Start Services:

- a Dimensions RM Common Tomcat
- b Dimensions RM Pool Manager
- c Terminate all running RM License Tool processes.

## Azure SAML2 Authentication

To register Dimensions RM as an Azure application:

- 1 Open the Azure portal in your web browser (<https://portal.azure.com>).
- 2 Log in with your administrative account, e.g. *admin@usernamedomain.onmicrosoft.com*.



**IMPORTANT!** There is help available on the Azure portal, please refer to on-line instructions to configure a Web application.

- 3 Select **App registrations**.
- 4 To access the client ID, click **Expose an API**
- 5 Copy and save the **Application (client) ID**, it will be used in web.xml as **Audience** value.
- 6 Select **Overview-->Endpoints**
- 7 Copy and Save **Login** and **Logout Endpoints**.
- 8 On the Overview tab click **Redirect URL**

- 9 Click **Add a Platform**, select **Web**.
- 10 Click **Add URL and enter your URL**, for example:  
https://ormtestit-rm05:8443/rtmBrowser/auth
- 11 Select **ID tokens**.
- 12 **Save your platform and return to the RM Server**
- 13 Stop Services:
  - a Open Text Tomcat Service
  - b Open Text Pool Manager
- 14 Copy *RM\_Install*\Common Tools **###\tomcat\#\webapps\rtmBrowser\WEB-INF\web.xml** to a backup - just to be safe.
- 15 Open *RM\_Install*\Common Tools **###\tomcat\#\webapps\rtmBrowser\WEB-INF\web.xml** with a text editor, e.g. Notepad.
- 16 Search for **SAML2 SSO Filter**
- 17 Modify as follows:
  - a Uncomment the filter section.
  - b Set filter-name, param-value to **true**
  - c Set **Audience** param-value to the value copied from **Application (client) ID**.
  - d Set the **login** and **logout** param-value to the saved **Login** and **Logout Endpoints**
  - e Save web.xml

```

<!-- ===== Start of SAML2 SSO Filter Configuration ===== -->
<filter>
  <filter-name>Saml2SSOFilter</filter-name>
  <filter-class>de.qm.rm.sso.SamlSSOFilter</filter-class>
  <init-param>
    <param-name>enabled</param-name>
    <param-value>true</param-value>
  </init-param>
  <!-- Audience (EntityID) in SSO Idp -->
  <init-param>
    <param-name>audience</param-name>
    <param-value>api://6090a8b5-dafc-4d8b-a9a3-d538126af2d7</param-value>
  </init-param>
  <!-- SAML2 sign-on endpoint -->
  <init-param>
    <param-name>login</param-name>
    <param-value>https://login.microsoftonline.com/b1977ad7-766d-4f7e-93e9-5c7150724f28/saml2</param-value>
    <!--param-value>https://sergiyabalin-dev.onelogin.com/trust/saml2/http-post/sso/6730b187-1e00-42ec-8704-086
  </init-param>
  <!-- SAML2 sign-out endpoint -->
  <init-param>
    <param-name>logout</param-name>
    <param-value>https://login.microsoftonline.com/b1977ad7-766d-4f7e-93e9-5c7150724f28/saml2</param-value> -->
  </init-param>

```

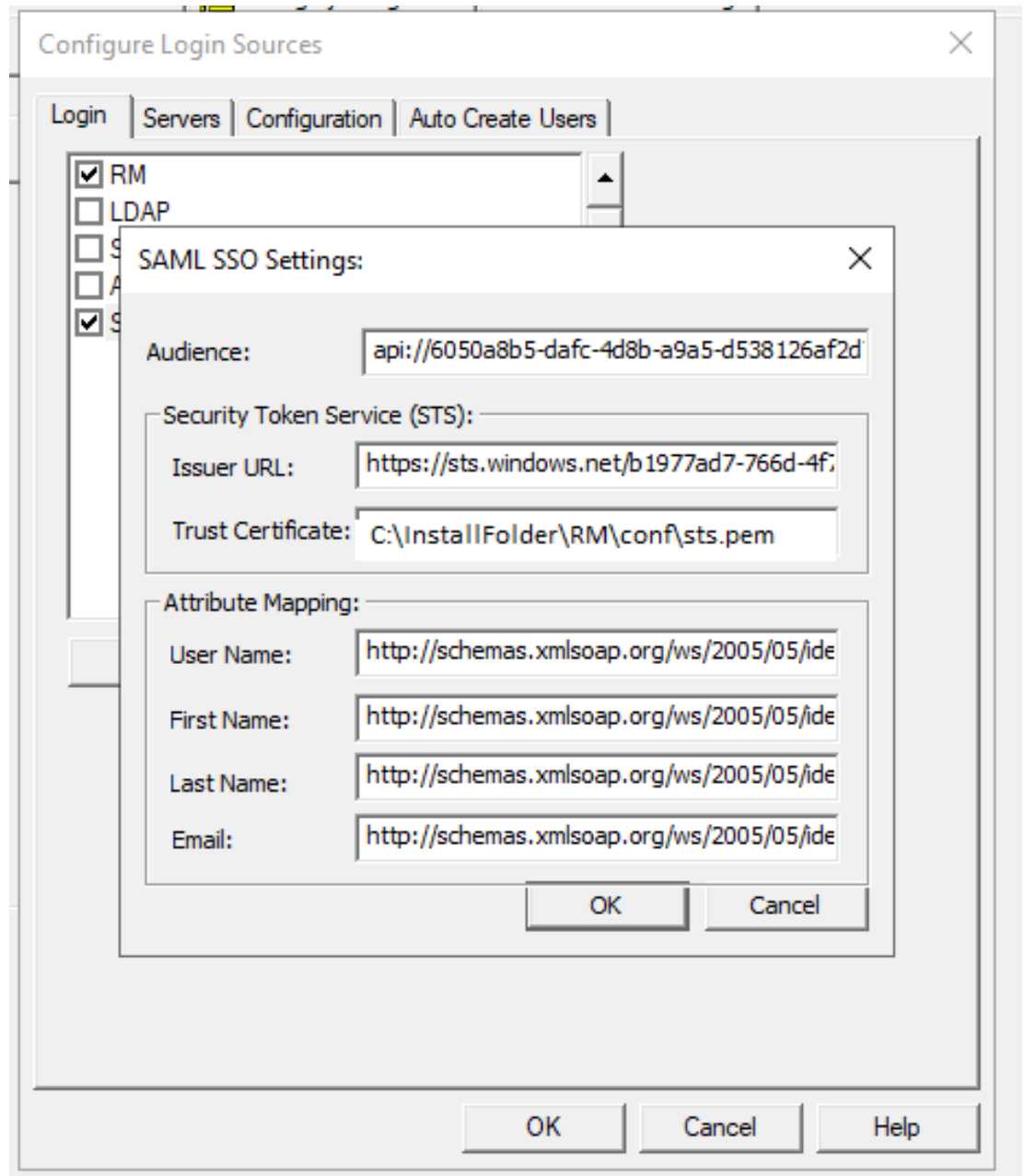
- 18 Configure login sources, checking **RM** and **SAML SSO** (see "[Specifying Login Sources in RM Manage](#)" on page 247). Enable Auto Create and add new user to default Instance and Group.
- 19 Settings for SAML SSO:
  - a Audience - same as that used in web.xml.
  - b Issuer URL - from Federation Server metadata.
  - c Trust certificate (copy value from Federation Server metadata to file sts.pem)

**20 To retrieve the Issuer URL, do the following:**

- a** Select **Azure Active Directory**.
- b** Select **App registrations**.
- c** Select **Endpoints**. This opens the list of endpoints.
- d** Copy the URL for the **Federation metadata document** into a new browser window. This loads an XML document.
- e** From the EntityDescriptor tag, copy the value of the **entityID** attribute. This is the Issuer URL.

**21 To retrieve the Issuer URL, do the following:**

- a** Select **Azure Active Directory**.
- b** Select **App registrations**.
- c** Select **Endpoints**. This opens the list of endpoints.
- d** Copy the URL for the **Federation metadata document** into a new browser window. This loads an XML document.
- e** From the EntityDescriptor tag, copy the value of the **entityID** attribute. This is the Issuer URL.



## 22 Start Services:

- a Open Text Tomcat Service
- b Open Text Pool Manager
- c Terminate all running rmLicenseAgent.exe instances in Task Manager

As with all Dimensions RM functionality, should you encounter issues, please contact Open Text support. If possible, provide screenshots.



# Appendix K

---

## Configuring Windows SSO

About Windows SSO	534
Configuring Windows SSO	534

---

## About Windows SSO

Windows SSO allows users to log-in through the web browser using their domain account, without specifying a password.

Note that not all web browsers support this feature "out of the box." For client applications, e.g. RM Manage, or RM Import, Windows SSO is not supported.

## Configuring Windows SSO



### **IMPORTANT!**

The Windows SSO.zip file is no longer included with the Dimensions RM distribution. Should you wish to install Windows SSO, please contact support for instructions.

If upgrading a current implementation of Windows SSO, please see the installation Guide.

# Index

---

## Symbols

!= constraint 313  
= constraint 313

## Numerics

2FA 258

## A

access rights  
    granting 219  
    revoking 221  
accounts, Oracle 47  
Acrobat Reader 468  
Add a Comment dialog box, omitting Role menu  
    from 270  
administrator, adding to instance 217  
Adobe Reader 468  
Agile  
    creating classes 80  
    creating relationships 93  
    enabling 94  
ALF. See Application Lifecycle Framework  
ALM integration 43  
alphanumeric attribute 277  
Amazon cloud 262  
animationspeed Web form option 53, 74  
Application Lifecycle Framework (ALF)  
    architecture 146  
    emitting events 147  
    enabling instances 150  
    event definition 149  
    event emitter 149  
    logging 155  
    overview 146  
    trigger points 148  
    Web services 149  
attribute constraints 339  
attributes  
    adding 295  
    alphanumeric 277  
    class 268  
    copying 297  
    Created by 276  
    date 278

    defining 295  
    deleting 298  
    description 237, 304  
    file attachment 278  
    for specific classes 270  
    group 279  
    Initial Created by 276  
    list 283  
    naming 27  
    non-unique names 237  
    numeric 290  
    overview 26  
    PUID 294  
    rqmt ID 294  
    text 291  
    title 237, 304  
    URL 291  
audit trail 37  
authenticator app 258  
Azure  
    registering 524  
    retrieving configuration data 525

## B

backing up  
    200  
    encrypted passwords 197, 198, 199, 200  
    legacy mode 198  
    normal mode 197  
baselines  
    setting link options 206  
Branching  
    creating classes 97

## C

cardinality 311  
categories  
    assigning permissions 221  
    naming 27  
    overview 36  
certificates  
    alias 439  
    CER format 352, 357, 432, 433  
    Federation Server 362  
    Gatekeeper 362

- importing into Tomcat 352, 357
  - keystore 439
  - PFX format 352, 357, 430, 434, 435, 439
  - server.xml 356
  - SSO 362
  - STS 362
  - change management 21, 43
  - changing database administrator account
    - password 225
  - changing the instance administrator password 231
  - chapter rules 407
  - checking
    - license server name 159
    - ORACLE\_HOME 159
    - security.dat file location 160
  - class attributes 268
  - class definition
    - overview 23, 266, 268
    - tasks 266
  - class definition diagram
    - canvas grid 272
    - centering 272
    - changing canvas size 272
    - editing instance header and footer 271
    - nudging objects 274
    - opening 270
    - ordering objects 274
    - panning 274
    - selecting objects 275
    - zooming 275
  - class image, changing 300
  - class rules 412
  - class types
    - adding 317
    - changing class definition bitmap 318
    - changing class icon 319
    - changing label properties 320
    - creating 301
    - defined 268
    - deleting 318
    - editing definition 318
  - classes
    - adding 299
    - changing class image 300
    - changing display properties 300
    - copying 301
    - creating class types 301
    - defining 302
    - deleting 301
    - naming 27
    - overview 25, 298
    - purging data 302
    - renaming 302
    - security transactions 322
    - specifying a description 305
  - collections
    - overview 42
  - comment class, defining to omit Role menu from
    - Add a Comment dialog box 270
  - constraint types 313
  - constraints 311, 313, 339, 340
  - contacting technical support 16
  - containers 42
  - containers, workflow
    - containers 346
  - conventions, typographical 15
  - convert database 201
  - convert instance 201
  - Created by attribute 276
  - creating classes
    - branching 97
    - merging 97
  - creating ICDBA account 161
  - creating new instances 164, 172, 175
  - current status 37
  - custom styles 61
  - customizing
    - menus in RM Browser 68
    - Web pages 50
  - customizing the Editable Grid 73
- ## D
- data structure 23
  - database administrator accounts
    - changing passwords 225
  - database administrator accounts unlocking 225
  - database conversion 201
  - database password encryption 235
  - database security 445
  - database upgrade 201
  - database validation 201
  - databases
    - converting 236
    - indexes 205
    - logging on 236
    - logging on as different user 236
    - managing 235
    - procedures 205
    - resources 205
  - date attribute 278
  - default access 224
  - default group access 218
  - default user access 219
  - deleting instance account 201
  - description attribute 237, 304
  - Dimensions CM
    - associating Dimensions RM containers to Dimensions CM projects/streams 261

- associating Dimensions RM instances to Dimensions CM products 261
    - logging into server 261
    - security 234
  - DOC file 468
  - Document 467, 468
  - documents
    - defining custom styles for exported documents 61
    - defining headers and footers for exported documents 65
    - exporting a document with file attachments from a separate server 67
  - Draft Requirements Document
    - append 382
    - import 383
    - save 382

## E

- Editable Grid, customizing 73
- emitter service
  - installing 153
  - options 152
  - usage 151
- enabling Agile 94
- encryption of database passwords 235
- Export 467, 468

## F

- file attachment attribute 278
- filters
  - overview 41
- form view 39

## G

- grid layout 40
- grid view 39
- group access, granting 320
- group attribute 279
- groups
  - administering 214
  - assigning users 216
  - changing group information 216
  - copying 215
  - creating 214
  - deleting 216
  - overview 24

## H

- headers and footers 65
- HTML formatting 291, 412
- HTML text editor 73

## I

- ICADMIN
  - changing password 227
  - unlock 230
  - updating password in security.dat 228
- ICADMIN, about 47
- ICDBA
  - changing password 225
  - unlock 226
- ICDBA account
  - creating 161
- ICDBA, about 47
- IIS
  - exporting CER certificates 433
  - exporting PFX certificates 435
  - importing PFX certificates 430
- impact analysis 42, 43
- Import, Draft Requirements Document 383
- Import, Word Document 378
- Initial Created by attribute 276
- instance
  - changing password 181
  - defining schema 202
  - dropping tables 205
- instance administrator password
  - changing 231
- instance conversion 201
- instance password, changing 181
- instance schema
  - backing up 202
  - defining 202, 266
  - deploying 324
  - overview 25
  - printing definitions 326
  - printing diagram 326
  - releasing lock 324
  - reloading 324
  - restoring from backup 203
  - saving 323
- instance tables
  - dropping 205
  - installing 204
- instance upgrade 201
- instances
  - backing up schema 202
  - converting 236
  - creating new 164, 172, 175
  - deleting instance account 201

- enabling ALF 150
- information 267
- installing tables 204
- placing account offline 204
- placing account online 204
- recreating database indexes 205
- recreating database procedures 205
- recreating database resources 205
- restoring account from backup 189
- restoring schema 203
- viewing assignment 214

Internet Information Services

- exporting CER certificates 433
- exporting PFX certificates 435
- importing PFX certificates 430

## L

LDAP

- configuring 252
- configuring to use SSL 256
- enabling SSL 257
- example configurations 254
- importing certificates 256
- specifying a server 252
- updating user information for all users 210

license server 159

Like constraint 314, 339, 342

link transfer rules 312

links

- overview 26

list attribute 283

list values, sorting 286

logging

- ALF 155

logging on, database 236

login sources

- specifying 247

## M

Management Console

- exporting CER certificates 432

menus, customizing 68

Merging

- creating classes 97

MMC

- exporting CER certificates 432

## N

naming classes, attributes, categories 27

Not Like constraint 314

numeric attribute 290

## O

objects

- overview 25

operations parameters 267

Oracle accounts 47

Oracle database security 446

ORACLE\_HOME 159

order of precedence 231

## P

paragraph layout 40

Password May be Incorrect in Security File or Security File May Not be Found error, resolving 466

password rules settings 223

password security 235, 258

passwords, sample databases 44

post processing

- Word document 491

PostgreSQL database security 463

pre-upgrade activities

- backing up your existing database 183, 185, 187, 189, 192, 194

previewing a document in RM Import Designer 424

printing manuals 16

process documentation 269

projects

- phasing 267

publish templates, creating 63

PUID attribute 294

## Q

QLARIUS\_RM sample database 44

queries

- overview 41

query terminology 41

## R

regular expressions, Word 425

relationship constraints 340

relationships

- adding 306
- cardinality 311
- changing display properties 306
- constraints 313

- defining 309
- deleting 307
- editing vertices 308
- overview 26, 269, 306
- purging data 308
- renaming 309
- reversing 309
- rules 269
- security transactions 323
- specifying a description 310
- specifying constraints 311
- transfer rules 312
- report transactions 235
- reports 21, 42
- requirement creation 36
- requirement development 20
- requirement evolution 37
- requirement lifecycle 38
- requirement rules 408
- requirement views 39
- requirements
  - copying 297
- requirements management 20
- resource types 218
- restoring
  - instance account 189
  - instance schema 203
- revoking access rights 221
- RM Browser
  - menus, customizing 68
- RM Import
  - configuration 388
    - security protocol 388
  - Excel
    - column mapping 384
    - import 388
    - import into document 387
    - import rules 386
  - Excel file 383
  - Import Draft Requirements Document 383
  - overview 22
  - Preview Dialog 380
  - Word Document 378
- RM Import Designer
  - Chapter Rules tab 407
  - Class Rules tab 412
    - attribute information 415
  - commands 403
  - creating a new template 404
  - deleting a template 405
  - General tab 406
  - logging in 401
  - opening a template 403
  - Preview tab 424
  - Requirement Rules tab 408
    - Keyword option 410

- Section option 409
- Table option 408
- Rules tab
  - class information 412
  - saving a template with another name 404
  - Word regular Expressions 425
- RM Import Designer Word Template examples
  - begin and end keyword 472
  - capturing title and description
    - no title rule 480
    - title rule 482
  - entire table with keyword 474
  - heading styles 479
  - section option with keywords 477
  - table option with every row 475
- RM Manage
  - overview 23
- RM Manage
  - Amazon cloud 262
- RMDEMO sample database 44
- Role menu, omitting from Add a Comment dialog
  - box 270
- rqmt ID attribute 294
- rules
  - populate attributes 315

## S

- sample databases 44
- scripts
  - overview 41
- Secure Socket Layers 352
- security
  - attribute transactions 232
  - best practice 320
  - categories 221
  - class transactions 232
  - collection transactions 233
  - database 445
  - database password encryption 235
  - default access 224
  - Dimensions CM projects 234
  - granting group access 320
  - groups 218
  - import transactions 234
  - Oracle database 446
  - order of precedence 231
  - overview 27, 223, 320
  - PostgreSQL database 463
  - relationship transactions 234
  - SQL Server 457
  - valid transactions 321
- security protocol
  - RM Import 388
- security.dat 235

- security.dat file 160
- server.xml 356
- setting
  - license server name 159
  - ORACLE\_HOME 159
  - security.dat file location 160
- setting link options for baselines 206
- Single Sign On 250, 251
- sorting list values 286
- source documents
  - security transactions 323
- special characters 258
- SQL Server database security 457
- SSL 388
- SSL. *See* Secure Socket Layers.
- SSO 250, 251
  - certificates 362
- strong password enforcement 258
- suspect links
  - implementing 327
  - security 323

## T

- tablespaces
  - administering 237
  - default size 171
  - dropping 238
  - placing online or offline 239
  - resizing 239
  - setting default location 239
- technical support
  - contacting 16
- template
  - creating 404
  - deleting 405
  - opening 403
  - saving
    - RM Import Designer
      - saving a template 404
    - saving with another name 404
- templates, creating 63
- Test Case Management 127
- text attribute 291
- title attribute 237, 304
- TLS 388
- Tomcat
  - importing certificates 352, 357
- traceability 21, 42
- traceability reports
  - overview 41
- transfer rules 312
- troubleshooting 465
- two-factor authentication 258
- typographical conventions 15

## U

- unlocking database administrator accounts 225
- upgrade database 201
- upgrade instance 201
- URL addressable views 486
- URL attribute 291
- URL syntax 486
- users
  - adding administrator 217
  - adding to a group 212
  - adding to an instance 216
  - administering 206
  - changing password information 212
  - changing user information 210
  - copying 208
  - creating new 206
  - deleting 210
  - deleting from an instance 223
  - overview 24
  - removing from a group 213
  - removing from instance 217
  - updating user information for all users 210

## W

- Web pages, customizing 50
- web server
  - importing PFX certificates 430
- Web service logging 132
- Web services
  - ALF 149
- Windows
  - importing PFX certificates 430
- Word Document
  - import 378
  - post processing 491
- Word regular expressions 425
- Word Template examples
  - begin and end keyword 472
  - capturing title and description
    - no title rule 480
    - title rule 482
  - entire table with keyword 474
  - heading styles 479
  - section option with keywords 477
  - table option with every row 475
- workflow
  - about 331
  - create 332
  - disable 345
  - edit 332
  - elements 332
- workflow state
  - add 333

- change definition 334
- change name 334
- delete 335
- settings
  - common 334
  - description 334
  - form 334
  - security 335
- workflow transition
  - add 336
  - change definition 336
  - change name 336
  - delete 344
  - settings
    - attribute constraints 339
    - description 337
    - form 337
    - relationship constraints 340
    - security 344

