MICRO FOCUS®

Dimensions® RM 12.10
Administrator's Guide

Table of Contents

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.
bold	Emphasizes important information and field names.
UPPERCASE	Indicates keys or key combinations that you can use. For example, press the ENTER key.
monospace	Indicates syntax examples, values that you specify, or results that you receive.
monospaced italics	Indicates names that are placeholders for values you specify; for example, *filename*.
monospace bold	Indicates the results of an executed command.

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

Printing Manuals

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

Contacting Technical Support

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

> http://supportline.microfocus.com

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

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

- Report problems and ask questions.

- Obtain up-to-date technical support information, including that shared by our customers via the Web, automatic e-mail notification, newsgroups, and regional user groups.

- Access a knowledge base, which contains how-to information and allows you to search on keywords for technical bulletins.

- Download fix releases for your Micro Focus products.

License and Copyright Information for Third-Party Software

For license and copyright information of third-party software included in this release, check the file `Third_Party_Licenses.txt`, which can be found in the Dimensions RM installation directory, e.g. C:\Program Files\Micro Focus\Dimensions 12.10\RM.

Chapter 1
Dimensions RM Overview

What is Dimensions RM?

Dimensions RM is the Micro Focus Software solution for requirements management. Dimensions RM delivers an enterprise-wide solution based on an Oracle® RDBMS or Microsoft SQL Server. Dimensions RM makes it easy for you to capture and organize requirements data by providing the tools you need to create, manage, and track such data throughout an instance's lifecycle.

What is 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.

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, comma separated value (CSV) file, or XML document (.xml) file. You synchronize Word documents or text documents with the database as requirements evolve.

You can also import requirements from other tools, such as Micro Focus Solution Business Manager (formerly known as Serena® Business Manager, Serena® Business Mashups and TeamTrack), IBM® Rational® Software Modeler, HP Quality Center, and Microsoft® Project. 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 user has the appropriate permissions, he or she can accept or reject the change request.

Communication

Dimensions RM provides several ways to facilitate communication among team members.

- **Comments**—You can participate in discussion threads by adding comments to requirements. This functionality allows you to communicate issues and discuss their resolution without directly changing the requirement.

  For information about adding comments in RM Browser, see the *Dimensions RM Browser User's Guide*.

- **Polls**—Users with the appropriate permissions can start a poll on a requirement. The poll typically either solicits feedback on its content or asks whether a change request against the requirement should be accepted or rejected. If the e-mail service is running, and the user accounts include e-mail addresses, the poll participants receive an e-mail message that notifies them about the poll and provides a direct link to the RM Browser page from which they vote. For more information on polling, see the *Dimensions RM Browser User's Guide*.

- **E-Mail Notification**—Users or administrators can set up rules that specify that an e-mail notification be sent when a particular event occurs. For example, you could set up a rule that causes an e-mail notification to be sent to you when any requirement you created changes.

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 Browser

RM Browser is the primary user interface. It provides Web access to a core set of Dimensions RM functions. Using RM Browser, both remote and local users can use a Web browser to edit requirements, submit and review change requests, run reports, create scripts, participate in discussions, run polls, create containers (baselines, collections, documents, or snapshots), manage categories, associate containers to Dimensions CM projects, and so on. RM Browser requires no installation.

RM Import
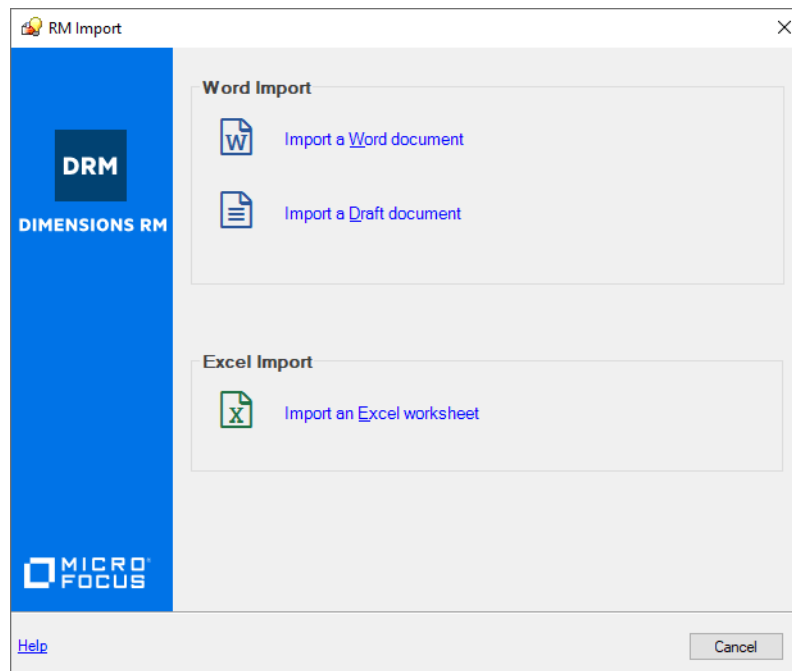
Figure 1-1. RM Import

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, move attributes between chapters, and so on. When satisfied with the draft document, users can import the document into Dimensions RM as a document. For detailed information about using RM Import, see chapter "RM Import" on page 395.

RM Import Designer
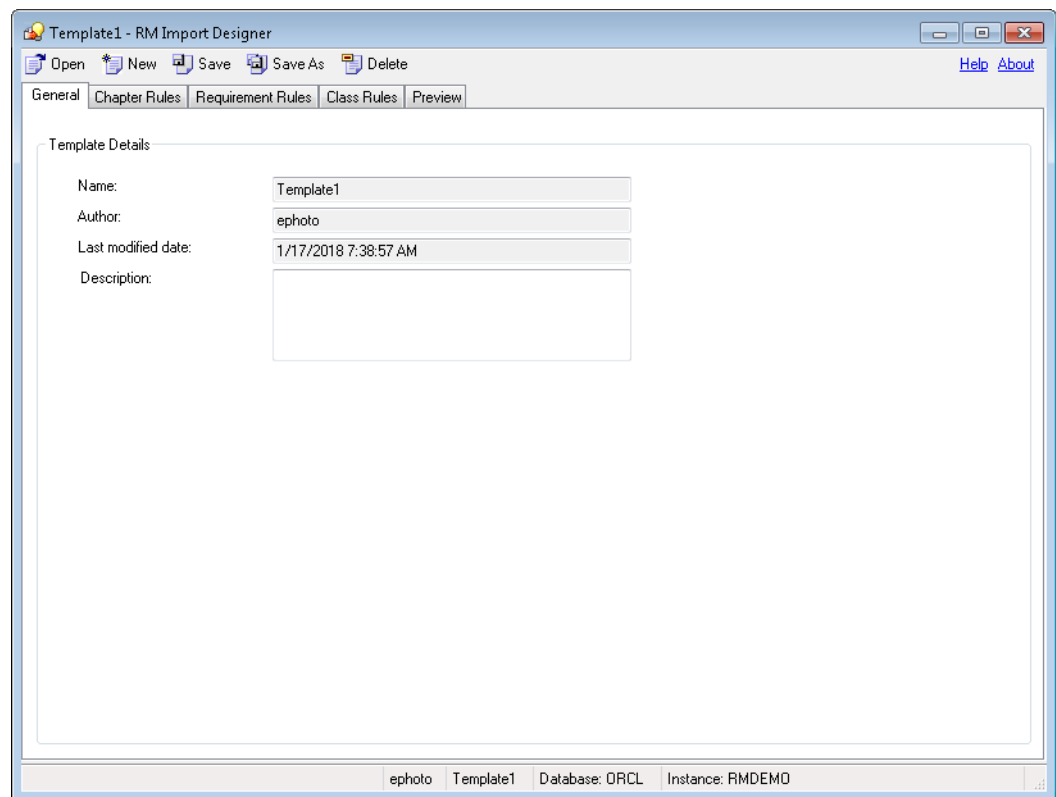
Figure 1-2. RM Import Designer

RM Import Designer allows administrators to design templates that users select 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. Administrators 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 411.

RM Manage
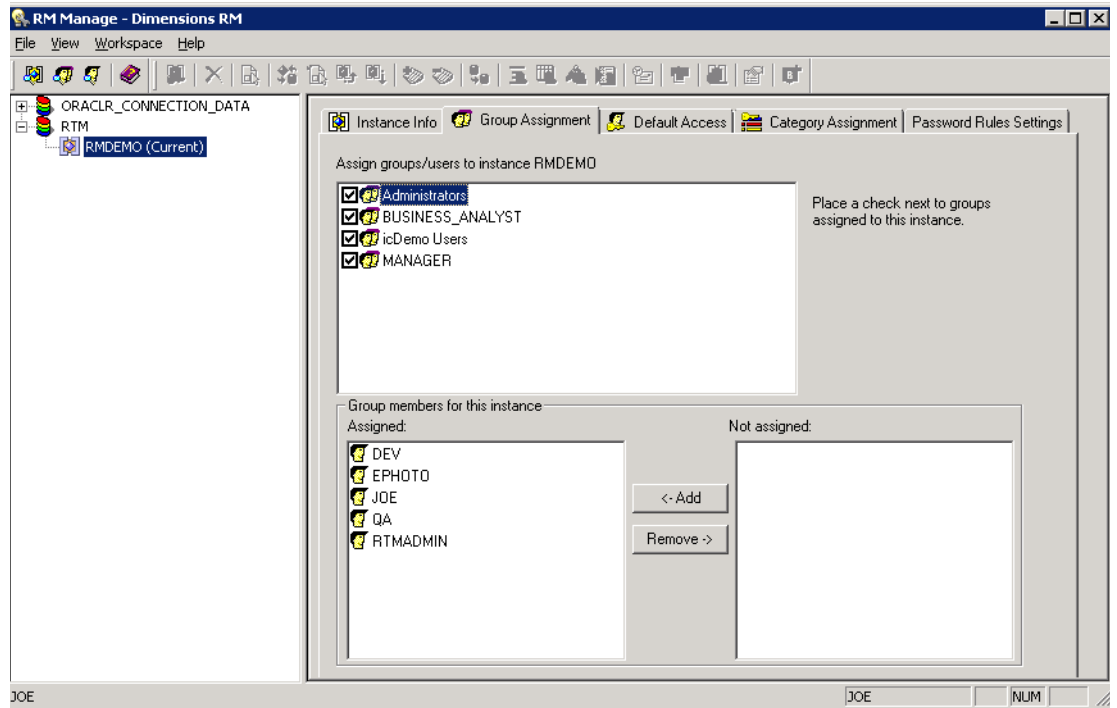
Figure 1-3. RM Manage

RM Manage allows instance administrators and instance admins to define users and groups, administer instance security, configure the instance database, organize data, and control user access and data routing. For detailed information about using RM Manage, see "RM Manage" on page 151.

Class Definition

Class Definition allows instance administrators to set up instance schemas in class definition diagrams. This involves defining classes, relationships, attributes, and security.

For detailed information about using Class Definition, see "RM Import Designer" on page 411.
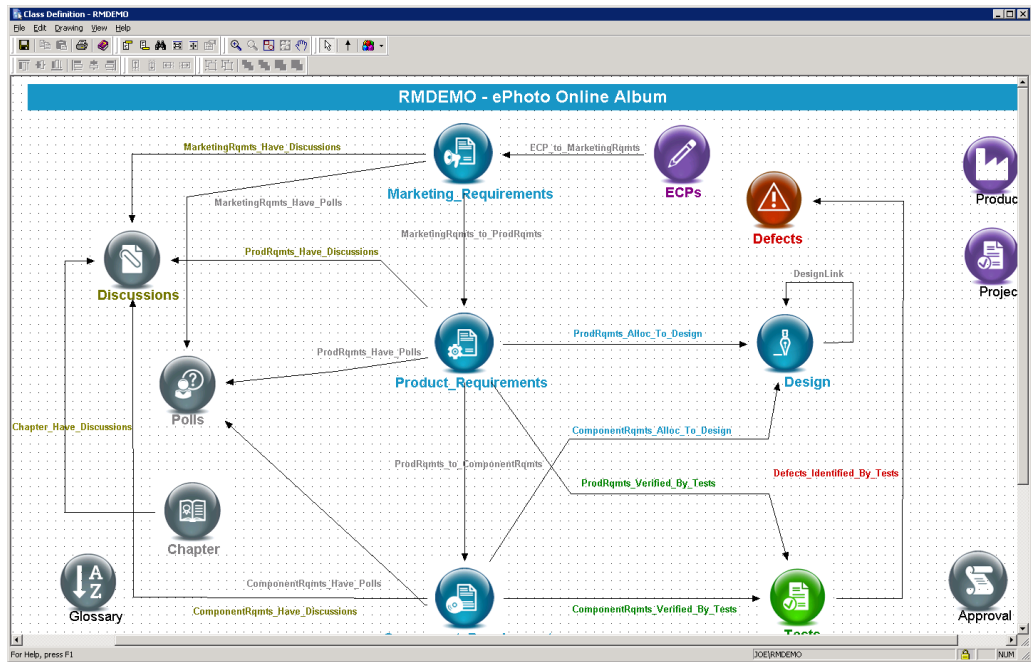
Figure 1-4. Class Definition

Dimensions RM Data Structure

The following diagram illustrates the Dimensions RM data structure.
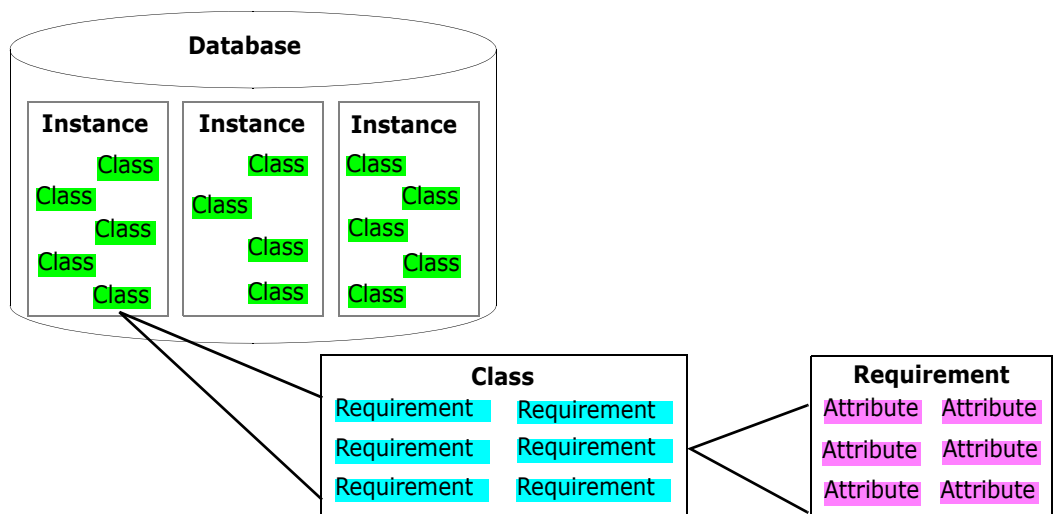
Figure 1-5. Dimensions RM Data Structure

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.

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

Dimensions RM Basics

This section provides an overview of basic Dimensions RM concepts.

Instances and Databases

Dimensions RM "instances" are the containers of related requirements and other engineering data along with the Dimensions RM customizations (forms, scripts, and so on) that users create to manipulate that data. The instance is the main focus of activity within Dimensions RM. Dimensions RM stores instances in an Oracle database or Microsoft SQL Server.

NOTE If you want to share requirements among projects, use categories to represent projects. For more information about categories, see "Categories" on page 38.

As a Dimensions RM user, you can access any number of instances and databases from the Dimensions RM tools. Each instance uses a single Oracle user account.

Administrators use the RM Manage tool to create and maintain instances. For information about RM Manage, see "RM Manage" on page 151.

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 the modifications made to the instance while the user is logged in to the account.

NOTE Dimensions RM user accounts are distinct from operating system user accounts and Oracle user accounts.

While access to instance elements can be controlled on a single-user basis, Dimensions RM users are typically organized into groups that can 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. Members of a pre-defined Administrators group can add additional members to the group.

Each Dimensions RM instance has a special user account, the instance admin. The instance admin is automatically and irrevocably granted privileges that allow him or her to manage the instance. Other users can be given administrative privileges at the discretion of the instance admin. The instance administrator and instance admin use the RM Manage tool to create and manage users and groups. For information about using the RM Manage tool, see "RM Manage" on page 151.

NOTE The instance admin is not part of the Administrators group.

Instance Schemas

Each Dimensions RM instance has its own schema that defines the kinds 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; you only need the classes and relationships that you will use now. As the instance evolves, other classes and relationships can be added and existing classes can be changed.

Schemas are created in a class definition diagram through the Class Definition tool. For an illustration of a class definition diagram, see "Class Definition" on page 24. For information about using Class Definition, see "RM Import Designer" on page 411.

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 processes that are to be supported. Common examples of classes include Marketing_ Requirements, Customer_Requirements, Security_Requirements, Software_Requirements, Hardware_Requirements, Action_Items, Test_Cases, and Engineering_Change_Proposals.

NOTE Words in class names must be connected with underscores.

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 *Use Cases*, *Customer Letter*, and *Business Justification* 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 *Pass*, *Fail*, and *Untested* as valid values for a list attribute named test_result.
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 □ 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 32).
- 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 32).

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 32).

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 32).

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

- Relation ship name must not be one of the reserved words (see "Reserved Words" on page 32).

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 *"About 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 Micro Focus Solution Business Manager (formerly known as Serena® Business Manager, Serena® Business Mashups and TeamTrack), IBM® Rational® Software Modeler, HP Quality Center, Microsoft® Project, and Microsoft® Excel®.

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 298.

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.
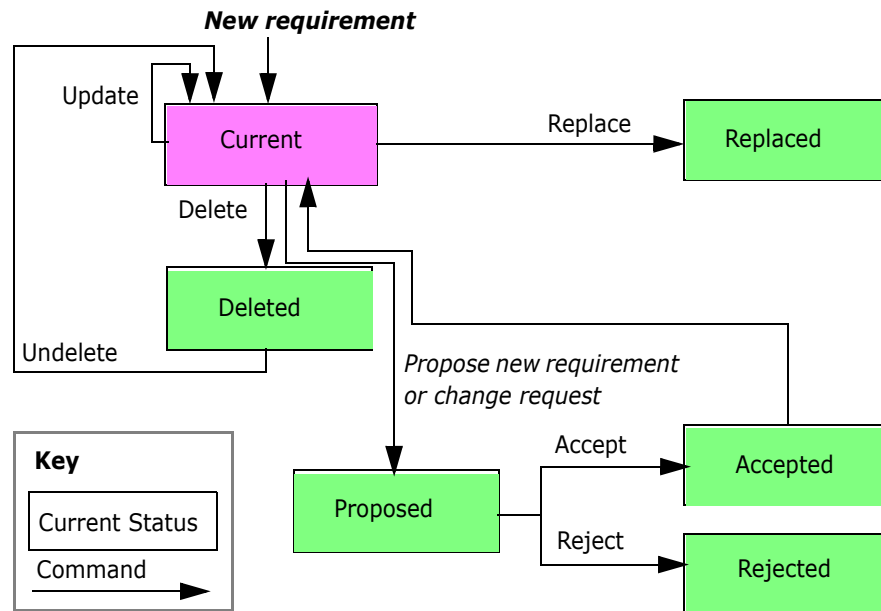
Figure 1-6. Object Lifecycle

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.

Figure 1-7. 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.

Figure 1-8. Grid View in RM Browser

Paragraph Layout

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

Figure 1-9. 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.

Figure 1-10. Grid Layout in Documents View of RM Browser

Queries

Queries are scripts, expressed in terms of the instance schema, that you use to retrieve selected objects. Scripts are queries against one or more classes. Traceabililty reports are queries based on relationships. Dimensions RM has an SQL-like language that handles input parameters and performs simple computations. In general, searches of instance data are based on selection criteria in which you specify constraints on attribute values and links.

The following describes scripts:

- **Scripts** can be used to combine the selection criteria capabilities, with complex link traversal, parameterization, basic calculations, and output formats. You can use any of these search mechanisms to locate data for review, modification, or export.

- **Traceability reports** are scripts that use relationships as the selection criteria. You specify a top-level class, and then select classes that have a relationship with the top-level class. You can constrain the report based on a container (baseline, collection, document, or snapshot) or category.

You can create and run scripts and traceability reports.

In Requirements View, you can use the quick search feature to quickly run a query to see the content of any category based on criteria you specify.

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 39, 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 Serena® Dimensions® 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 Databases

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.

> **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 Database

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 *(SQL Server only)*	Yes (Instance)

QLARIUS_RM		
User Name	**Password**	**Administrator**
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	qa	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
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	qa	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
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

Oracle Accounts Used by Dimensions RM

Dimensions RM uses three Oracle user accounts at the core of the product interface:

- ICDBA

- ICADMIN

Additional Oracle user accounts are created for each Dimensions RM instance, such as RMDEMO, QLARIUS, etc. Each new Dimensions RM instance is an Oracle database user account. The instance accounts are schema owners in Oracle. The RM Manage tool creates a new tablespace with an associated data file for each new instance (Oracle account) and assigns the default profile to it. Alternatively, for new RM instances, DBAs can create a tablespace then have RM Manage use that existing tablespace to install the schema etc. A profile other than the default can be set by DBAs after RM Manage creates the new instance/Oracle account.

! **IMPORTANT!** Special function profiles are not recommended for this purpose, such as BATCH_USER, as they may not allow real-time and transaction processing to occur correctly.

ICDBA Account

Dimensions RM only uses the SYS account to create the Oracle user: ICDBA. After that, all SYSDBA functions are performed by ICBDA. ICDBA creates new instances (named oracle users) in new or user selected tablespaces. When the first instance is created, the additional Oracle user account ICADMIN is created.

Dimensions RM is designed not to require an Oracle Database Administrator (DBA); the RM administrator can perform the necessary Oracle maintenance functions without having to access Oracle directly.

However, large customers with Oracle DBAs on staff can simply reset the ICDBA password after the system is in production and allow the DBA staff to perform the Oracle maintenance tasks. After initial system setup, configuration, and verification, access to the ICDBA account is rarely needed if DBAs perform the Oracle maintenance tasks. For the rare occasion where the ICDBA account is needed in RM, the DBA simply enters the password in the RM client.

For shops without a DBA staff, Dimensions RM administrators would use the ICDBA account to perform Oracle Maintenance tasks.

For information on creating the ICDBA account, see "Creating the ICDBA Account" on page 154.

Oracle Account Password Management

ICADMIN, and RM instance account (RMDEMO, QLARIUS, etc.) passwords are managed and maintained by Dimensions RM. Note that passwords are case sensitive. In addition, Dimensions RM has its own password rules (see "Setting Password Rules" on page 276).

TIP Department of Defense customers, and others with a requirement for mixed-case passwords, can compensate for the lack of case-sensitive passwords by increasing the minimum length of the passwords by four characters.

The ICDBA account is managed by Oracle and must conform to the rules of your Oracle installation. Oracle can use a mixed-case password for the ICDBA account.

It is recommended that these accounts be set to never expire or lock. Then, on a regular basis, use RM Manage to change the ICADMIN, and RM instance account passwords. RM administrators will not receive the Oracle notice that the account is about to expire. As a result, the RM administrator must remember to change the account password before they expire or they will be locked out of the system. Once locked out due to password expiration, it is challenging to get the Oracle password changed while RM learns the new password. Dimensions RM stores these passwords for application access using 3DES security with the option for customer supplied keys.

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

You can customize the RM Browser Web forms and dialog boxes that contain Dimensions RM attribute fields. To perform the customization, you edit an XML file to create a user-defined template.

In this section, when *attribute* is cited, it refers to Dimensions RM attributes, not JavaScript attributes.

The following list specifies the things you can do to customize Web forms and dialog boxes (referred to as *forms* in the remainder of this section):

- Change the order of attributes within a section.

- Specify the attributes to be included in a section.

- Create a subgroup of the attributes within a section. This subgroup can be a group box or an expandable heading that contains the attributes.

- Add a button, hyperlink, or other HTML element to the form that is linked to an external source that may return values to Dimensions RM fields.

- Add your own sections and distribute attributes among them however you prefer.

- Change the number of columns that a section uses to lay out the attributes.

- Change or hide lists in query-style forms (for example, the operator list).

The user-defined template consists of an XML file that contains sections for the global items contained in the form (for example, scripts, cascading style sheets [CSS], and so on), dialog sections and their order, and the order of fields within each section.

NOTES

- If you hide attribute controls through JavaScript, attribute controls following the hidden attribute controls may be re-arranged. This may be confusing to some users. If and how attribute controls a re-arranged depends on the method you use for hiding these attribute controls.

- The user-defined template is described in detail in "Template Layout" on page 55.

Template Processing

A templates directory (*RM_Install*\Common Tools *#.#*\tomcat*#.#*\webapps \rtmBrowser\forms) contains all the template files for the 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, an entire instance, or all instances.

The templates are processed as follows:

1   RM Browser looks for a class-specific XML file, and loads it if it is 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 (forms\common\default.xml). This file creates a standard Dimensions RM appearance.

The naming of the database and instance directories 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
<?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.

```
                    <?xml version="1.0" encoding="UTF-8"?>
1 ──────────────<form xmlns="http://schemas.serena.com/2005/01/rtmform" animationspeed="5">
2 ─────────────<script src="../jscript/myCustomScript.js"/>
3 ─────────────<stylesheet src="../cssmyCustomStylesheet.css"/>
4 ─────────────<section type="user" label="My First Section" cols="3" labelplacement="top">
5 ───────────<attribute id="ACTUAL_FIX_TIME"/>
                    <attribute id="DESCRIPTION" colspan="2"/>
6 ──────────<group label="Release Information" cols="2" labelplacement="left"
                     expandable="no">
                       <attribute id="RELEASE_ID" label="Id"/>
                       <attribute id="RELEASE_DATE" label="Date"/>
                       <attribute id="RELEASE_STATUS" label="Status"/>
                    </group>
7 ─────────────<text><![CDATA[<a href="http://www.serena.com"><img src="http://
                     www.serena.com/Images/logos/serena.gif"></a>]]></text>
                    </section>
                    <section type="user" label="My second Section" cols="2">
                       <attribute id="RESPONSIBLE_ANALYST" type="Custom" label="Analyst"
                       colspan="2">
8 ──────────────<writeable>
9 ──────────────<xhtml>
                           <input name="myField" type="text" value="" size="30" maxlength="10"
                    onchange="dosomethingspecial()" onfocus="dosomethingspecial()" />
                           <button type="button" id="myButton"
                    onclick="dosomethingspecial()">Search...</button>
                       </xhtml>
                       </writeable>
                    </attribute>
                    </section>
                    <section type="prioritized"/>
                    <!--
                    <section type="standard" label="Standard Attributes"/>
                    <section type="custom" label="Custom Attributes"/> -->
                    <section type="groupattribute" label="Group Attributes"/>
                    <section type="system" label="My System"/>
                    <section type="attachments" label="File Attachments"/>
                    <section type="comments" label="Discussions"/>
                    <section type="links" label="Relationships"/>
                    <section type="history" label="History"/>
                    <section type="polls" label="Polls"/>
                    <section type="dimensions" label="Dim CM Associations" />
                    <section type="container"/>
                    </form>
```

CAUTION! Attributes can only be defined in one section.

Tag	Description
1	Sections in forms are set by default to open and close by a scrolling mechanism. The `animationspeed` option determines one of the following: ■ The speed of the scrolling (default `animationspeed=0`) ■ Whether the scrolling mechanism is used. If it is not used (`animationspeed=0`), the sections open and close immediately when the user clicks **+** or **-**. For information about how to configure the `animationspeed` option, see "Configuring the Expansion and Collapse of RM Browser Sections" on page 78.
2	The `<script>` tag contains a user-defined JavaScript file. You can include more than one JavaScript file. 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 `onload`, `onunload`, `onfocus`, and `onblur` events. These are dialog specific and occur after the form finishes its own processing of these events. The function names for each form follow: **New Requirement**, **Edit Attributes**, **Change Request**, **Comments**, **Form View, Documents View**: `objOnLoad`, `objOnUnload`, `objOnFocus`, `objOnBlur`, `objHistoryOnLoad` (**NOTE:** The Documents View form is displayed only after you click a requirement in the navigation tree.) **Query by Class**, **Query by Relationship**: `queryOnLoad`, `queryOnUnload`, `queryOnFocus`, `queryOnBlur` **Edit Query:** `editQueryOnLoad` (**NOTE:** 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.) **Link Objects**: `linkOnLoad`, `linkOnUnload`, `linkOnFocus`, `linkOnBlur` **Organize by Collection**: `collOnLoad`, `collOnUnload`, `collOnFocus`, `collOnBlur` **Approve Change Request**: `crOnLoad`, `crOnUnload`, `crOnFocus`, `crOnBlur` **Organize by Category**: `catOnLoad`, `catOnUnload`, `catOnFocus`, `catOnBlur` **Add to Chapter**: `atcOnLoad`, `atcOnUnload`, `atcOnFocus`, `atcOnBlur`
	There are other JavaScript functions that you can use with query-style forms and other forms that contain attributes. See "Query-Style Form Functions" on page 59 and "Helper Functions" on page 62 for details.
	The `rtmObjCustomHtmlPrint(attrName)` function is called for any custom HTML attribute to get the read-only (print) value. The `attrName` parameter is the internal attribute name. 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. This function applies to the **New Requirement** and **Edit Attributes** dialog boxes only.
3	The `<stylesheet>` tag contains a user-defined stylesheet. You can include more than one stylesheet tag.

Tag	Description
4	The `<section>` tag contains either a predefined section or a user-defined section. 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. Predefined section types include standard, custom, system, attachments, comments, links, history, polls, and dimensions. Predefined section types are used in the template (.xml) file. You can rearrange the placement of these sections. 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. 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.
5	The `<attribute>` 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. You can specify a custom attribute type. RM Browser automatically generates a hidden attribute associated with a custom field by using the `attribute id` that is provided. You can specify how many columns the field consumes (defaults to one). See the description for tag 9 for options when you use XHTML/HTML inside an `<attribute>` tag.
6	The `<group>` tag allows you to physically group attributes, but in the confines of a section. A section could have several different groupings of attributes. 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).
7	The `CDATA` element can be used in `<text>` and `<attribute>` 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.

Tag	Description
8	The `<writeable>` 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 `<read-only>` 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. You have three options when you use XHTML/HTML: ■ The custom XHTML/HTML can apply to both editable and read-only forms (if specified directly inside the `<text>` or `<attribute>` tag). ■ Different XHTML/HTML can be provided for editable as opposed to read-only forms (if specified in `<writeable>` and `<read-only>` elements inside the `<text>` or `<attribute>` tag). ■ The XHTML/HTML can only apply to editable forms (if specified in `<writable>` only elements inside the `<text>` or `<attribute>` tag). With this option, read-only forms display the attribute in the standard way. The `<writeable2>` tag and `<readonly2>` tag are the same as the `<writeable>` tag and `<readonly>` tag, except that they are used whenever a range control is shown (any query-style dialog when **between** or **not between** is the selected operator). If these tags are not present, then the `<writeable>` tag and `<readonly>` 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.

9	The `<xhtml>` tag can be used in `<text>` and `<attribute>` tags. It allows you to insert XHTML-compliant code that adds elements such as buttons to the form.
	You can also add text boxes inside `<xhtml>` tags with sizes set to any number of columns and rows, optionally with scrolling. For example, the following tag:
	`<xhtml>`
	`<TEXTAREA name="New_custom11" id="new_id11" rows="4" cols="25" wrap="off">`
	`</TEXTAREA>`
	`</xhtml>`
	Adds a text box that allows four rows and 25 columns (in characters). The wrap="off" attribute enables scrollbars for this text box.

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
rtmQueryOnOperatorSelection (attrId, operator)	Called whenever an operator is selected in any query-style dialog. This function must return true if the selection is allowed or false if it is not allowed.
rtmQueryOnValueOptionSelection (attrId, option)	Called whenever a value option is selected in the list that opens to the right of the attribute control (**Query by Class** and **Query by Relationship** only). This function must return true if the selection is allowed or false if it is not allowed.
rtmQueryAddCustomAttribute Operators(attrId)	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 rtmQueryAdd... functions, or may simply call one of them to get the same list. The rtmQueryAdd... functions are listed below: ■ rtmQueryAddAlphaOperators ■ rtmQueryAddNumericOperators ■ rtmQueryAddDateOperators ■ rtmQueryAddListOperators ■ rtmQueryAddTextOperators and are defined in icObjectFormsMenus.js (located in *<RM Install Dir>*\rtmBrowser\rm\common\js). To customize the operator list, use the rtmQueryAdd... 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 rtmQueryLike and rtmQueryIn.
rtmQueryAddCustomAttribute Operators(attrName)	Called for custom attributes when a query constraints dialog box that contains that attribute is opened.
rtmQueryGetCustomValues(attrId, operator)	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 null for any attributes using the default processing.

Function	Description
rtmQuerySetCustomValues(attrId, values)	Called to set **in** and **not in** 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.
rtmQueryShowValueOptions (attrId)	Called to tell Dimensions RM to not show the list that opens to the right of the attribute control and contains the **Fixed** or **Entered at runtime** options.

Query-Style Form Function Parameters

The parameters for the "Query-Style Form Functions" on page 59 are described in the following table.

Parameter	Description
attrId	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 **Constraints-Source** or **Constraints-Target** tabs on the **Query by Relationship** form.
operator	A string with the internal operator (LIKE, IN, INITIALIZED, and so on) or pseudo-operator (BETWEEN and NOT BETWEEN).
option	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).
values	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
`rtmUtilGetAttributeElementId` `(attrId, isRangeCtrl)`	Builds an ID string based on the attribute name and the context from which it is being called. This function is not validated.
`rtmUtilGetAttributeValue` `(attrId, isRangeCtrl)`	Gets the value of the specified attribute from the Web form. If the element (as determined by `rtmUtilGetAttributeElementId`) 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.
`rtmUtilSetAttributeValue` `(attrId, value, isRangeCtrl)`	Sets the value of the specified attribute.

Helper Function Parameters

The parameters for the "Helper Functions" on page 62 are described in the following table.

Parameter	Description
`attrId`	The attribute name. This parameter is used to uniquely identify an attribute.
`value`	A string value to put into the Dimensions RM attribute in the Web form. This parameter does not work for non-Dimensions RM attributes.
`isRangeCtrl`	Valid values are `true` or `false`. This parameter is used with ranges (`BETWEEN` and `NOT BETWEEN`) that have two controls for a single attribute. The parameter would be `true` 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. **NOTE:** 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*\Common Tools *#.#*\tomcat*#.#*\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\Common Tools *#.#*\tomcat*#.#*\webapps\rtmBrowser\conf\
        Database_Name*Instance_Name*

    b **With a specific publish template:** Create the marked directories in path
    RM_Install\Common Tools *#.#*\tomcat*#.#*\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 54).

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.

Priority:	<PRIORITY>	**Delivery Phase:**	<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 65 and "Defining Headers and Footers for Exported Documents" on page 69.

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 70.

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 67 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 54).

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.microfocus.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>
```

<u>Button with Picture:</u>

```
<sct:largeButtonItem href="javascript:customFunction()">
  <img src="/rtmBrowser/myimages/logo.png" width="16" height="16">
  <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.

<u>Simple Menu:</u>

```
<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.microfocus.com')">Micro Focus Homepage
    </sct:subMenuItem>
  </sct:subMenu>
</sct:largeButtonItem>
```

<u>Menu with Tool Tips:</u>

```
<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.microfocus.com')">
              <span title="Go to the Micro Focus homepage.">Micro Focus
Homepage</span>
            </sct:subMenuItem>
          </sct:subMenu>
        </sct:largeButtonItem>
```

Menu with Picture:

```
<sct:largeButtonItem>
  <img src="/rtmBrowser/myimages/logo.png" width="16" height="16">
  <span>Custom Menu</span>
  <sct:subMenu>
    <sct:subMenuItem href="javascript:customFunction()">Custom Entry
    </sct:subMenuItem>
    <sct:subMenuItem href="javascript:window.open('https://
www.microfocus.com')">Micro Focus Homepage
    </sct:subMenuItem>
  </sct:subMenu>
</sct:largeButtonItem>
```

> **NOTE** After changing the `toppanel.jsp` file, you must restart the **Micro Focus 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 **Micro Focus 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 **Micro Focus 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.ja` 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 55.

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 in the following directory on the RM server:

    RM_Install\Common Tools *#.#*\tomcat*#.#*\webapps\rtmBrowser

    ■ If your users use Internet Explorer: warning.html (make sure that the file extension is .html, **not** .htm)

    ■ If your users use Firefox: warning.txt

2   Add the text to these files. If you used Microsoft Word to edit the HTML file for Explorer, you must save 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 you to add your 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 `spring.xml` file. It is on the server in the following location:
   RM_Install\Common Tools *#.#*\tomcat*#.#*\webapps\rtmBrowser\WEB-INF

2 Open the spring.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 footer here...* with the path to your header or footer file. The recommended directory is the `html` folder under `rtmBrowser`.

   For example:

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

   Then, the URL property value would be:
   `<property name="URL"><value>/rtmBrowser/html/securityheader.htm</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 RM's Tomcat service (Micro Focus Common Tomcat).

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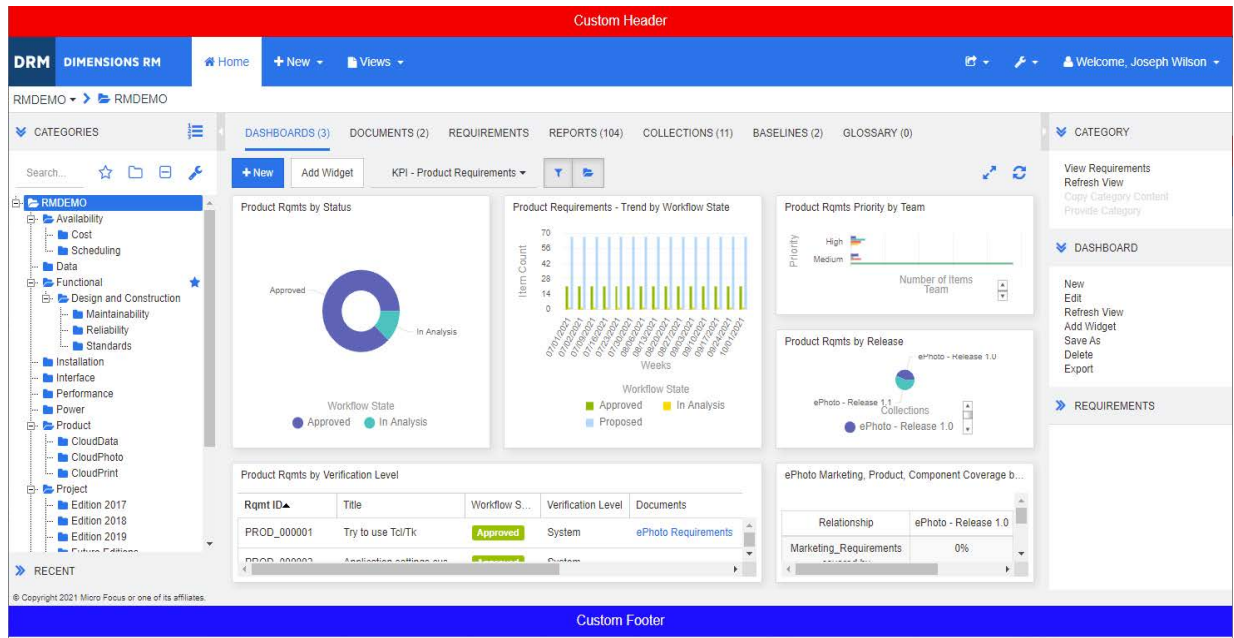
Dashboard Export

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 runningDimensions 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 `DashboardExport.exe.config` 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).

Format	Description
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

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 292.

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
Assigned To	User	**Attribute Mandatory**: No **Attribute Editable**: Yes **Force Unique Value**: No **Display For Entry**: Yes **Populate On Copy**: Yes **Populate On Create And Link**: Yes **Change Raises Suspicion**: No **All instance users**: Yes **All users from selected groups**: No **Specific users**: No **Allow multiple selections**: No
Description	Text	**Attribute Mandatory**: No **Attribute Editable**: Yes **Force Unique Value**: No **Display For Entry**: Yes **Populate On Copy**: Yes **Populate On Create And Link**: Yes **Change Raises Suspicion**: Yes **HTML Formatting**: Yes **Append Only:** No **Insert Newest First:** No
Name	Alphanumeric	**Attribute Mandatory**: Yes **Attribute Editable**: Yes **Force Unique Value**: No **Display For Entry**: Yes **Populate On Copy**: Yes **Populate On Create And Link**: Yes **Change Raises Suspicion**: Yes
Priority	List	**Attribute Mandatory**: No **Attribute Editable**: Yes **Force Unique Value**: No **Display For Entry**: Yes **Populate On Copy**: Yes **Populate On Create And Link**: Yes **Change Raises Suspicion**: Yes **List Entries:** ■ High ■ Medium ■ Low **Default Value:** Medium **Allow multiple selections:** No **Tag list:** No **Show as checkbox:** No

Features Class

Attribute Name	Attribute Type	Options
Assigned To	User	**Attribute Mandatory**: No **Attribute Editable**: Yes **Force Unique Value**: No **Display For Entry**: Yes **Populate On Copy**: Yes **Populate On Create And Link**: Yes **Change Raises Suspicion**: No **All instance users**: Yes **All users from selected groups**: No **Specific users**: No **Allow multiple selections**: No
Description	Text	**Attribute Mandatory**: No **Attribute Editable**: Yes **Force Unique Value**: No **Display For Entry**: Yes **Populate On Copy**: Yes **Populate On Create And Link**: Yes **Change Raises Suspicion**: Yes **HTML Formatting**: Yes **Append Only:** No **Insert Newest First:** No
Name	Alphanumeric	**Attribute Mandatory**: Yes **Attribute Editable**: Yes **Force Unique Value**: No **Display For Entry**: Yes **Populate On Copy**: Yes **Populate On Create And Link**: Yes **Change Raises Suspicion**: Yes
Priority	List	**Attribute Mandatory**: No **Attribute Editable**: Yes **Force Unique Value**: No **Display For Entry**: Yes **Populate On Copy**: Yes **Populate On Create And Link**: Yes **Change Raises Suspicion**: Yes **List Entries:** ▪ High ▪ Medium ▪ Low **Default Value:** Medium **Allow multiple selections:** No **Tag list:** No **Show as checkbox:** No

Products Class

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

Releases Class

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

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

Sprints Class

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

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

Stories Class

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

Attribute Name	Attribute Type	Options
Name	Alphanumeric	**Attribute Mandatory**: Yes **Attribute Editable**: Yes **Force Unique Value**: No **Display For Entry**: Yes **Populate On Copy**: Yes **Populate On Create And Link**: Yes **Change Raises Suspicion**: Yes
Planning Status	List	**Attribute Mandatory**: Yes **Attribute Editable**: Yes **Force Unique Value**: No **Display For Entry**: Yes **Populate On Copy**: Yes **Populate On Create And Link**: Yes **Change Raises Suspicion**: Yes **List Entries:** ■ Elaborated ■ Pre-Planning ■ Sprint-Ready **Default Value:** Elaborated **Allow multiple selections:** No **Tag list:** No **Show as checkbox:** No
Priority	List	**Attribute Mandatory**: No **Attribute Editable**: Yes **Force Unique Value**: No **Display For Entry**: Yes **Populate On Copy**: Yes **Populate On Create And Link**: Yes **Change Raises Suspicion**: Yes **List Entries:** ■ High ■ Medium ■ Low **Default Value:** Low **Allow multiple selections:** No **Tag list:** No **Show as checkbox:** No

Attribute Name	Attribute Type	Options
Ranking	Numeric	**Attribute Mandatory**: No **Attribute Editable**: Yes **Force Unique Value**: No **Display For Entry**: Yes **Populate On Copy**: Yes **Populate On Create And Link**: Yes **Change Raises Suspicion**: Yes
Remaining Effort	Numeric	**Attribute Mandatory**: No **Attribute Editable**: Yes **Force Unique Value**: No **Display For Entry**: Yes **Populate On Copy**: Yes **Populate On Create And Link**: Yes **Change Raises Suspicion**: Yes
Spent Effort	Numeric	**Attribute Mandatory**: No **Attribute Editable**: Yes **Force Unique Value**: No **Display For Entry**: Yes **Populate On Copy**: No **Populate On Create And Link**: Yes **Change Raises Suspicion**: Yes
Sprint Status	List	**Attribute Mandatory**: Yes **Attribute Editable**: Yes **Force Unique Value**: No **Display For Entry**: Yes **Populate On Copy**: Yes **Populate On Create And Link**: Yes **Change Raises Suspicion**: Yes **List Entries:** ■ Not Started ■ In Development ■ In Test ■ In Review ■ Accepted **Default Value:** Not Started **Allow multiple selections:** No **Tag list:** No **Show as checkbox:** No

Tasks Class

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

Attribute Name	Attribute Type	Options
Priority	List	**Attribute Mandatory**: No **Attribute Editable**: Yes **Force Unique Value**: No **Display For Entry**: Yes **Populate On Copy**: Yes **Populate On Create And Link**: Yes **Change Raises Suspicion**: Yes **List Entries:** ■ High ■ Medium ■ Low
Task Status	List	**Attribute Mandatory**: Yes **Attribute Editable**: Yes **Force Unique Value**: No **Display For Entry**: Yes **Populate On Copy**: Yes **Populate On Create And Link**: Yes **Change Raises Suspicion**: Yes **List Entries:** ■ To Do ■ In Progress ■ In Test ■ Done

Creating Relationships

After creating the classes, you need to create relationships between the classes.
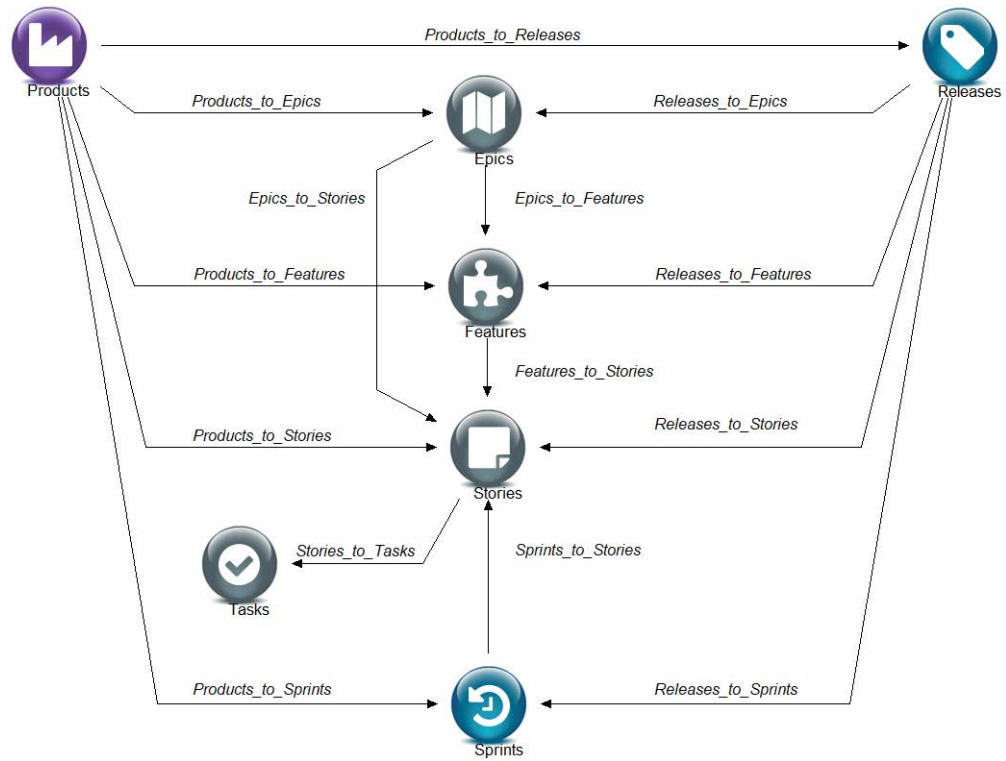
To create the relationships follow these steps:

1 Start the Class Definition tool as described in chapter "Starting Class Definition" on page 292.

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 *Release*s to *Sprints*.

k From *Release*s 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 Sub-Categories

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 sub-category. 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

Some functions in Dimensions RM are not enabled by default, e.g. because special classes must be created. The following chapters describe how to enable these special functions.

Agile

Please refer to chapter .

Branching and Merging of Requirements

In order to use branching and merging of requirements, a Product and a Project class needs to be added to the class definition.

To add the classes, follow these steps:

1   Start the Class Definition tool as described in chapter .

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 ![save] in the toolbar.

Documents

In order to use documents, a Chapter class needs to 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 292.

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 ![save] in the toolbar.

Glossary

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 292.

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 ![save] in the toolbar.

Test Case Management

Please refer to chapter "Test Case Management" on page 119.

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

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

To install the chatbot, execute these steps:

1 Install the Rasa server version 2.8.10 following the official installation instructions at <ins>https://rasa.com/docs/rasa/2.x/installation</ins>.

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\Micro Focus\Dimensions 12.10*\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.yml`.

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 104.

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 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\Micro Focus\Dimensions 12.10*\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

Before you continue

You must insure that the chatbot is installed either by executing the steps from chapter "Manual Installation" on page 102, or from chapter "Docker Image Installation" on page 103.

To configure the chatbot, execute these steps:

1 In Windows Explorer, navigate to *RM_INSTALL*\RM\conf, e.g. *C:\Program Files\Micro Focus\Dimensions 12.10*\RM\conf.

2 Open the file chatbot.properties with Notepad or another plain text editor.

3 For the enabled setting, change the value to **true**, so the line reads enabled=**true**.

4 For the host setting, change the value to your server name or IP address your Rasa server is running on, e.g. host=*myrasaserver*.

5 If you changed the port during the installation, change the value for the port setting to the new port, e.g. port=*6006*.

6 Save the file.

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

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 105). 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 105)

3 Restrict groups by IP addresses (see chapter "Restricting Groups by IP Addresses" on page 107)

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 105.

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 105)

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 105.

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 105)

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 105
>
> ■   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 105)
>
> ■ 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 there IP addresses as described in chapter "Restricting Groups by IP Addresses" on page 107.

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 Micro Focus Single Sign On (SSO) option in the Dimensions RM installer installs components needed for the RM server to communicate with a Micro Focus SSO server. The Micro Focus SSO server is an optional part of a Dimensions CM or SBM installation.

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

Configuring SSL Certificates

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

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

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

> **NOTE** To communicate with the Micro Focus SSO server (STS server), your RM Server and fat client systems must include a copy of the STS server certificate.
>
> See "Exporting a Certificate from IIS" on page 110, "Exporting a Certificate from the STS Server" on page 110 and "Adding a Certificate for RM Server to the STS Keystore" on page 110.

■ Create a certificate for the RM web server (RM_WEB_CERT). To enable SSO with remote fat clients, the RM web server should be configured for SSL and the certificate should be signed by a known certificate authority.

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

Exporting a Certificate from IIS

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

> **NOTE** The following example procedure shows how to export a CA certificate from IIS server. However, as of Dimensions RM 12.1, Dimensions RM includes its own Tomcat web server, so Apache and IIS are not required, though you can optionally run a third-party web server in addition to the Micro Focus Common Tomcat web server if you wish to avail yourself of the security and management features of a third-party web server.

1 Retrieve the certificate in CER format by following the steps in chapter "Exporting Certificates to CER Format from IIS" on page 453.

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 457 or "Exporting the STS Certificate from SBM Configurator" on page 458.

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

2 Copy the resulting *sts.pem* file to *RM_Install*\RM\conf (e.g. *C:\Program Files\Micro Focus\Dimensions 12.10*\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 113.

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 452 or "Exporting Certificates to CER Format from IIS" on page 453.

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\Micro Focus\Dimensions 12.10*.
>
> ■ Replace **#.#.#.#** with the Common Tools version number, e.g. *1.8.6.0*.
>
> ■ Replace **#.#** with the Java version number, e.g. *11.0*.
>
> The complete set command may look like this:
>
> `set path=%path%;"`*`C:\Program Files\Micro Focus\Dimensions`* `12.10\Comm on Tools `*`1.8.6.0`*`\jre\`*`11.0`*`\bin"`

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

> **NOTE** Starting with SBM version 2009R4.01, truststore.jks contains a demo Dimensions RM server certificate. If you import your own certificate with the suggested alias **rmserver**, type the following command and press **Enter**:
>
> `keytool -delete -alias rmserver`
> `-keystore truststore.jks -storepass `*`StorePassword`*
>
> ■ Replace *StorePassword* with the password for the keystore.
> The default password for the truststore.jks keystore is: **changeit**

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

NOTE

- Replace *TruststoreName* with the file name of the truststore. The default is truststore.jks. If the keystore name contains spaces, surround it with double quotes.

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

- Replace *Alias* with a unique name.
  Suggested aliases:

  - rm_ca for a CA certificate.

  - rmserver for the RM server certificate.

- Replace *CerPath* with the full path to your certificate in CER format. If the path contains spaces, surround the path with double quotes.

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

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

Enabling SSO as a Login Source

Before you can use SSO authentication with RM instances, you must enable SSO as a login source for the database that contains them. The SSO login source is enabled via the RM Manage interface. See the *Dimensions RM Administrator's Guide* for details.

Registry Keys and Configuration Files on the RM Server

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

RM Server Parameters

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

RM Server Registry Keys	
Key	**Description**

RMKey
(String)
	Contains a full path to a file with a private key of the RM server certificate. The Key file should not be password protected. The file must be in .pem format.
	Example:
	<pre>C:\Program Files\Micro Focus\Dimensions 12.10
	    \RM\conf\rmkey.pem</pre>

RMCertificate
(String)
	Contains a full path to a file for a certificate of the RM server. The file must be in .pem format.
	Example:
	<pre>C:\Program Files\Micro Focus\Dimensions 12.10
	    \RM\conf\rmcert.pem</pre>

SSOServer (String)	Contains the URL to the SSO/STS server. Only the host name and port are required. Example: <pre>http://ssohost:8085</pre>
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:
	<pre>C:\Program Files\Micro Focus\Dimensions 12.10
	    \RM\conf\sts.pem</pre>

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

Gatekeeper Parameters

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

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

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

gatekeeper-core-config.xml	
Parameter	**Description**

SecurityTokenService	URL to the STS server. This is configured by the installer.
	Example:
	`http://sts-server:8085/TokenService/`
	`services/Trust`

SecurityTokenServiceExternal	Same as the SecurityTokenService.
FederationServerURL	URL to the Federation server. This is configured by the installer. Example: `http://sts-server:8085/ALFSSOLogin/login`

gatekeeper-services-config.xml	
Parameter	**Description**
Path: <GatekeeperProtectionControl> <ProtectedURIs> Element: <URIMatcher requestURI="/rtmBrowser/*" />	URIMatcher should have one line that contains "/rtmBrowser/*" string. This is a definition of a filter to protect a particular web application.
Path: <Service name="default" ProtectionLevel="all"> <ServiceEntryPoints> <BrowserRequests> Element: <URIMatcher requestURI="/rtmBrowser/*" />	Protected URL mask.

gatekeeper-services-config.xml	
Parameter	**Description**
Path: <GlobalLogoutURI> Element: <URIMatcher requestURI="/*/logout-sso.jsp" />	The default logout URL to use with the sequence to invalidate SSO token. When accessing this URL, the Gatekeeper automatically rejects the SSO token causing the login screen to appear.
Path: <DMZ> <BrowserRequests> Elements: <URIMatcher requestURI="/rtmBrowser/css/*"/> <URIMatcher requestURI="/rtmBrowser/html/*"/> <URIMatcher requestURI="/rtmBrowser/images/*"/> <URIMatcher requestURI="/rtmBrowser/imagesnew/*"/> <URIMatcher requestURI="/rtmBrowser/jscript/*"/> <URIMatcher requestURI="/rtmBrowser/jscripts/*"/> <URIMatcher requestURI="/rtmBrowser/WebServices"/> <URIMatcher requestURI="/rtmBrowser/WebServices/rtmService.wsdl"/> <URIMatcher requestURI="/rtmBrowser/Command"/>	

Registry Keys and Configuration Files on the Fat Client

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

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

RM Fat Client Registry Keys	
Key	**Description**
RMKey (String) (Optional)	Contains a full path to a file with a private key of the RM server certificate. The Key file should not be password protected. The file must be in .pem format. Example: `C:\Program Files\Micro Focus\Dimensions 12.10\RM\con f\rmkey.pem`
RMCertificate (String) (Optional)	Contains a full path to a file for a certificate of the RM server. The file must be in .pem format. Example: `C:\Program Files\Micro Focus\Dimensions 12.10\RM\con f\rmcert.pem`
SSOServer (String)	Contains the URL to the Dimensions CM or SBM SSO/STS server. Only the host name and port are required. Example: `http://ssohost:8085`

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

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

Troubleshooting

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

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

2   LDAP Server unavailable

If you are using LDAP with SSO, check that the LDAP server is available. With SBM, you perform this check with the SBM Configurator.

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\De fault`.

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\De fault`.

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**.

Chapter 5
Test Case Management

Overview

The following section describes the setup up for Test Case Management using Dimensions RM. Test Case Management provides the facility for the definition of special classes, designed to test related solutions within RM.

The test management classes, Test_Case and Test_Run, like all classes in Dimensions RM, may be modified once created using the default definition.

Class Definition

To implement Test Case Management as defined below, two classes must first be defined: Test_Case and Test_Run. These classes can be named using your organization's convention for naming classes; for simplification this document is using the default names *Test_Case* and *Test_Run*.

Creating Test Management Classes from Templates

Dimensions RM brings templates for the Test Case and Test Run classes. These class templates simplify the process of setting up Test Management. To create a custom class or modify your existing class, see chapter "Using Custom Classes with Test Management" on page 121.

To create the classes, follow these steps:

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 | Test Case** from the shortcut menu.

6 Click on a free space to place the new class.

7 Change the name to your liking, e.g. Test_Case.

8 Right-click on a free space and select **Add Class | Test Run** from the shortcut menu.

9 Click on a free space to place the new class.

10 Change the name to your liking, e.g. Test_Run.

11 Save the class definition.

12 Execute the steps in chapter "Setting the Default Value for Test Steps" on page 121.

13 Execute the steps in chapter "Creating a Relationship between the Test Management Classes" on page 122.

Using Custom Classes with Test Management

If using a custom class with Test Management, it is essential that the classes *Test_Case* and *Test_Run* have the **Test Steps** attribute.

To modify a class for Test Management, follow these steps:

1   Create a class or use an existing class in your class definition.

2   Double-click the class you just created or the existing class you want to modify.

3   Click the ⊤ button.

4   Enter *Test Steps* into **Display Name** box.

5   Ensure that the **Attribute Name** box contains **TEST_STEPS**.

6   Select the **Text** tab.

7   Ensure that the **HTML Formatting** box is selected.

8   Open the file *RM_Install*\RM\tutorial\TestManagement\TestStepForm.html with a text editor.

9   Copy the html code between
     `<!-- please copy this html into the form -->`
        and
     `<!-- end of text for Form -->`
        to the Clipboard.

10   Paste the copied HTML code into the **Default Value** box.

11   Click **OK** to close the **Definition of attribute** dialog.

12   Click **OK** to close the **Definition of class** dialog.

13   Save the class definition.

Setting the Default Value for Test Steps

In order allow entering test steps, the **Test Steps** property needs to provide the user interface. This requires to set the default value of the **Test Steps** property for classes *Test_Case* and *Test_Run*.

To set the Default Value, follow these steps:

1   Open the file *RM_Install*\RM\tutorial\TestManagement\TestStepForm.html with a text editor, e.g. Notepad.

2   Copy the html code between `<!-- please copy this html into the form -->` and `<!-- end of text for Form -->` to the Clipboard.

3   Double-click the class *Test_Case*.

4   On the **Attributes** tab, expand the **User Defined** folder.

5   Double-click the **Test Steps** property.

6   Select the **Text** tab.

7   Ensure that the **HTML Formatting** box is selected.

8   Paste the previously copied HTML code into the **Default Value** box.

9   Click **OK** to close the **Definition of attribute** dialog.

10   Click **OK** to close the **Definition of class** dialog.

11   Double-click the class *Test_Run*.

12   Repeat steps 4 through 10 for the class *Test_Run*.

13   Save the class definition.

Creating a Relationship between the Test Management Classes

In order to connect a test case and one or several test runs, it is required to create a relationship between the classes Test_Case and Test_Run.

To create the relationship follow these steps:

1   Click the ↑ button in the toolbar.

2   Select class **Test_Case**.

3   Select class **Test_Run**.

4   Name the relationship, e.g. Test_Case_Has_Test_Runs.

5   Double-click the relationship arrow or right-click the relationship arrow and select **Define** from the shortcut menu.

6   Select the **Constraints** tab.

7   For Primary Links and Secondary Links, ensure that these check boxes are selected:

- transfer to child
- populate attributes on create and link

8   Click **OK**.

9   Save the class definition.

Forms

For the Test Case Management functionality it is required that the classes use forms. The forms are located under this path:
RM Install\Common Tools *#.#*\tomcat*#.#*\webapps\rtmBrowser\forms which will be referred to as *RM Forms*.

Creating Forms for Test Management

The following steps describe how to create a form if no form for the desired class exists. If you use a class for which a form already exists, see chapter "Modifying Forms for Test Management" on page 123.

Follow these steps to create a form:

1 If it does not exist, create the directory DataBase_Name in this directory:
RM Install\Common Tools *#.#*\tomcat*#.#*\webapps\rtmBrowser\forms.

> **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 Copy the file *RM Install*\RM\tutorial\TestManagement\Test_Case.xml into this directory:
RM Install\Common Tools *#.#*\tomcat*#.#*\webapps\rtmBrowser\forms*Database_Name**Instance_Name*.

4 Rename the file Test_Case.xml to resemble the name of your class, but keep the .xml file extension.

> **IMPORTANT!** The class needs to have the Test Steps attribute.

5 Copy the file *RM Install*\RM\tutorial\TestManagement\Test_Run.xml into this directory:
RM Install\Common Tools *#.#*\tomcat*#.#*\webapps\rtmBrowser\forms*Database_Name**Instance_Name*.

6 Rename the file Test_Run.xml to resemble the name of your class, but keep the .xml file extension.

> **IMPORTANT!** The class needs to have the Test Steps attribute.

Modifying Forms for Test Management

When using an existing class for Test Management, you might need to add the Test Management functionality to an existing form.

To modify the form of your Test Case class, follow these steps:

1 In Windows Explorer, navigate to this directory:
RM Install\RM\tutorial\TestManagement

2 Open the file Test_Case.xml in a text editor, e.g. Notepad.

3 Select the code between the <form> tag and the first <section> tag and copy it to the Clipboard.

4 In Windows Explorer, navigate to this directory:
RM Install\Common Tools *#.#*\tomcat*#.#*\webapps\rtmBrowser\forms*Data base_Name**Instance_Name*

NOTE *Database_Name* and *Instance_Name* are identical with the database name and instance name from the login dialog.

5 Open the XML file which resembles the name of the class that handles test cases, e.g. Test_Case.xml, with a text editor like Notepad.

6 Paste the code you copied to the Clipboard into your XML file between the `<form>` tag and the first `<section>` tag.

7 Save the file.

To modify the form of your Test Run class, follow these steps:

1 In Windows Explorer, navigate to this directory:
RM Install\RM\tutorial\TestManagement

2 Open the file `Test_Run.xml` in a text editor, e.g. Notepad.

3 Select the code between the `<form>` tag and the first `<section>` tag and copy it to the Clipboard.

4 In Windows Explorer, navigate to this directory:
RM Install\Common Tools *#.#*\tomcat*#.#*\webapps\rtmBrowser\forms

5 Open the XML file which resembles the name of the class that handles test runs, e.g. Test_Run.xml, with a text editor like Notepad.

6 Paste the code you copied to the Clipboard into your XML file between the `<form>` tag and the first `<section>` tag.

7 Save the file.

Chapter 6
Logging

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 128.

- 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 127.

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 128.

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 log4jappenderfile<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 128.

■ 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 128.

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 128.

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.	■ ERROR
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.	■ ERROR ■ WARN

Log Level	Description	Log Levels included in Log File
INFO	Provides general information about an operation.	■ ERROR ■ WARN ■ INFO
DEBUG	Provides step-by-step information about an operation. Debug is the highest level of logging.	■ ERROR ■ WARN ■ INFO ■ DEBUG

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 128.

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 134.

- **Remove** operations delete data of a certain age from both tables. See "Remove Operations" on page 135.

- **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 136.

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 130 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 130 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

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:

- Micro Focus Solution Business Manager Composer—A 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 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.
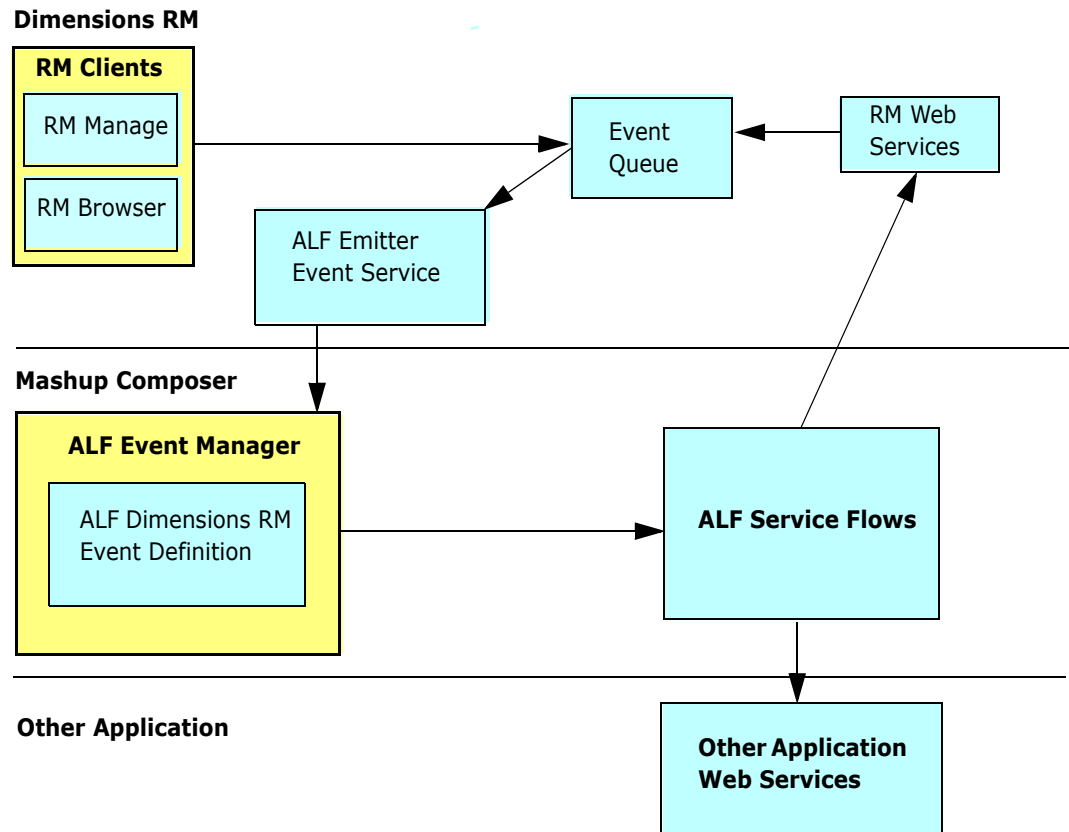

Figure 7-1. Integration Architecture

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 144.

The following flowchart illustrates the process of emitting an event from Dimensions RM.
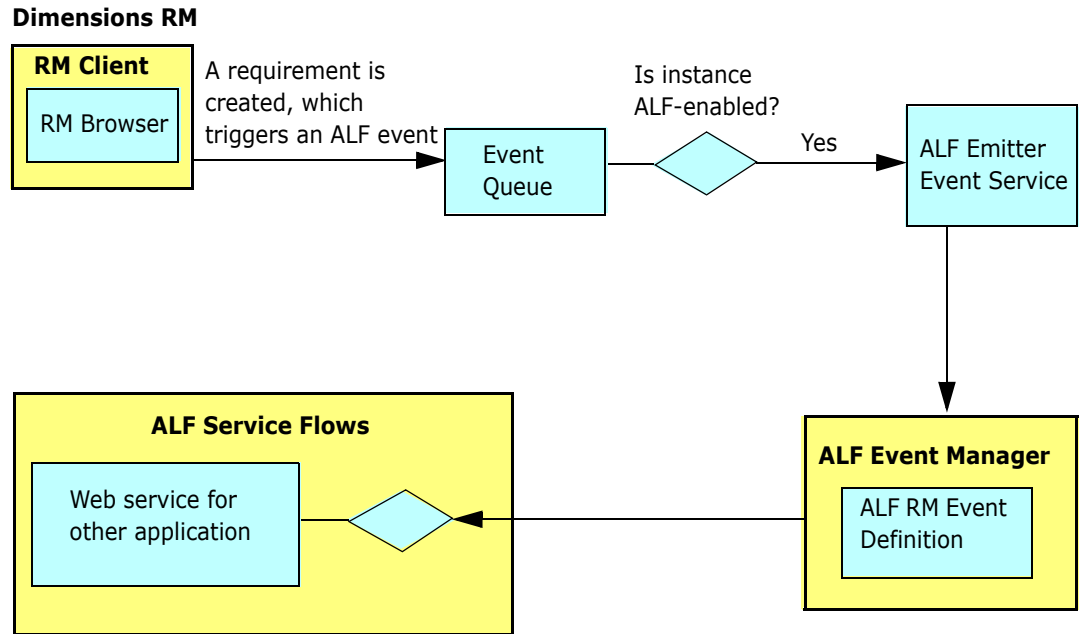
Figure 7-2. Emitting an Event from Dimensions RM

> **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 149.

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 145.

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 Micro Focus Support Web site.
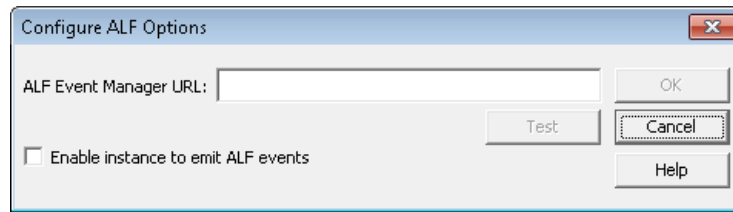
Enabling an Instance for ALF

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

Installation

To install the emitter service, user 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 Micro Focus 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.

For further information about logging, see chapter "Logging" on page 125.

Troubleshooting

Micro Focus ALF Event Emitter Service Fails on Startup

If the **Micro Focus 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 146.

Chapter 8
RM Manage

Overview

RM Manage is the Dimensions RM tool for administering databases and instances. With Oracle RDBMS, the data is organized by Oracle instances (databases) and Oracle users (instances). With MS SQL Server, the data is organized by SQL Server instances (databases). You can access the user and group data through separate views in the RM tool.

Only the databases in the Oracle "tnsnames.ora" file are displayed in the graphical tree in the left window. This file is located in the following sub-directory of the top-level installation directory of the Oracle RDBMS:

- Local or Remote Windows RDBMS

    NETWORK\ADMIN

- Remote UNIX RDBMS

    network/admin

To access instances in a database, you must first log in using a valid Dimensions RM administrator ID and password. When you have been authenticated for a database, the instances for which you have been assigned as an administrator are displayed as subfolders of the database. Any tools launched from RM Manage use the current user, password, database, and instance settings.

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

Configuration

The following sections describe how to view current configuration settings or specify new ones for Dimensions RM.

> **NOTE** Configuration information that is stored in the registry during installation can be changed after installation.

Setting RTM_HOME

RTM_HOME must be set to the Dimensions RM installation directory if it is not already correctly set by default. This value is stored in the registry and is used to locate the executables for other Dimensions RM tools.

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

To check or set RTM_HOME:

1   In **RM Manage**, select **Workspace | Options**.

2 Click the **Mandatory** tab.

3 In the **RTM_HOME** field, if currently incorrectly set, enter the location of Dimensions RM or browse to the Dimensions RM installation directory.

4 Click **Apply**.

Setting ORACLE_HOME

ORACLE_HOME must be set to the Oracle installation directory if it is not already correctly set by default. This value is stored in the registry and is used to determine the top-level installation directory of or your company's Oracle RDBMS (which 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 ORACLE_HOME:

1 In **RM Manage**, select **Workspace | Options**.

2 Click the **Mandatory** tab.

3 In the **ORACLE_HOME** field, if currently incorrectly set, enter the location of Oracle or browse to the Oracle installation directory (for example, `C:\Oracle\ora10g`).

4 Click **Apply**.

Setting the License Server

The license server setting defines how licenses are requested:

- **Server:** The license setting is used for RM Browser client, RM Import, Class Definition, and web service requests.

- **Admin tool:** The license setting is used for Class Definition only.

To check or set the license server:

1 In **RM Manage**, select **Workspace** | **Options**.

2 Select the **License** tab.

3 **License Tool:** Specifies which licensing application is used. Only **Micro Focus AutoPass Licensing** is supported.

4 **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.

> **NOTE**
>
> ■ If you have 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. As there are no concurrent licenses, this request will fail.
>
> ■ 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.

5 **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.

6 Click **Apply** to save any changed license server settings.

Setting 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 an administrator changes the default location of this file, you will be requested to modify the location.

To check or set the location of the security.dat file:

1 Open RM Manage.

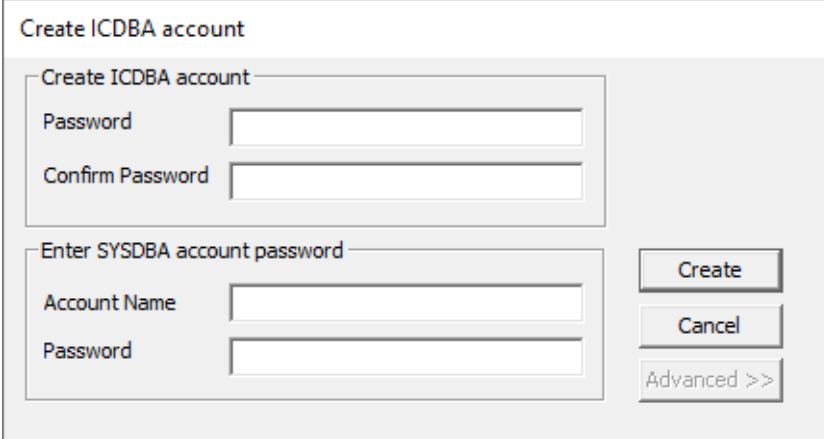> **NOTE** You do not need to log into Dimensions RM to perform this task.

2 Select **Workspace | Options**.

3 The **Workspace Options** dialog opens.

4 Click the **Security** tab.

5 In the **Security File** dialog box, if currently incorrectly set, type the full path to the `security.dat` file or browse to it.

6 Click **OK**.

Creating the ICDBA Account

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 [icon],
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.

8 By default, the ICDBA account is created in a new SERENA_RM_ADMIN tablespace for
the ICDBA account and its size is set to 1024 MB. To set a different size or create the

ICDBA account in an existing tablespace, click the **Advanced** button. The dialog expands to display the advanced features.

■ To set a different size for the SERENA_RM_ADMIN tablespace, set the **Tablespace** and **Units** values as desired.

■ To create the ICDBA account in an existing tablespace, select the **Create in existing tablespace** option, and select the desired tablespace from the list.

■ If you wish to resize one of the tablespaces or create a new one with a specific name, click the **Administer Tablespaces** button and complete the fields as necessary.

9 Click **Create**.

> **IMPORTANT!** For the Oracle RDBMS, Oracle account passwords expire by default after 180 days. Unless your DBA has re-configured such RDBMS to override this default and allow permanent passwords, you must to change the ICDBA password before 180 days elapse using the RM Manage **Change Administrator Password** menu item, see "Database Administrator Accounts: Changing Passwords and Unlocking" on page 222.

Managing Instances

Dimensions RM allows you to administer instances and databases through the RM Manage and Class Definition tools. You can perform all administrative tasks, including setting up and configuring directories, creating instances, setting up user accounts and passwords

and restoring instances from backup. Using the Class Definition tool, you can organize information according to types and define the attributes for each type.

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

Creating a New Instance with Oracle 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.

> **IMPORTANT!**
>
> - You must ensure that you create the ICDBA account (as explained in "Creating the ICDBA Account" on page 154) 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.
>
> - For the Oracle RDBMS, 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 ICADMIN password before 180 days elapse using the RM Manage **Change Administrator Password** menu item, see "Database Administrator Accounts: Changing Passwords and Unlocking" on page 222.

If the `ICADMIN` user has not been created, the **Enter ICADMIN password** dialog box opens.

Execute the following steps in this dialog:

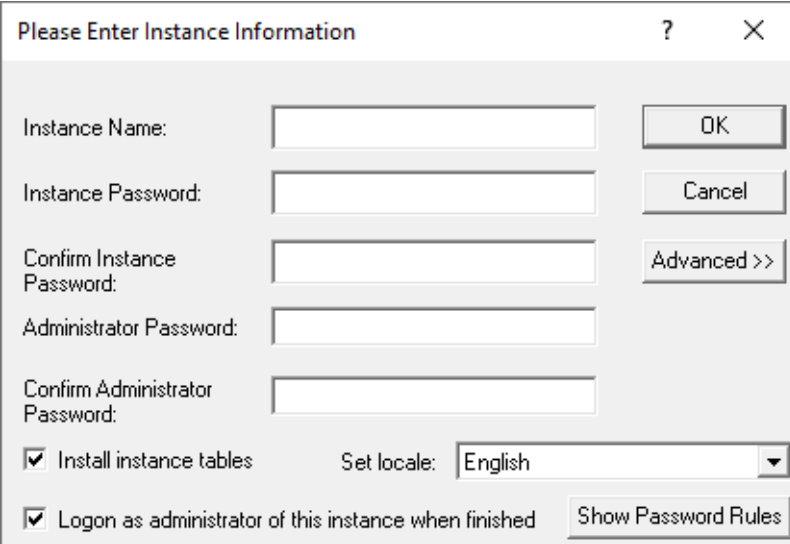**a** In the **ICADMIN Password** field, type the password to be assigned that account.

> **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). **CAUTION!** The instance name must follow the conventions specified in chapter "Naming Conventions for Instances" on page 30.
Instance Password	Enter an instance password (for example, MYINSTANCE). This password is used by Dimensions RM to access Oracle. RM users do not use it directly in Dimensions RM. **NOTE** Instance passwords cannot begin with a number. For example, 12345 causes an error; however, a12345 is accepted. Click **Show Password Rules** for a summary of the rules.
Confirm Instance Password	Re-enter the instance password.
Administrator Password	Enter a password for the instance's administrator account. You will need this password to administrate the instance. **NOTE** The ID for this account is the instance name with Admin appended to the end, for example MyinstanceAdmin. This account only has access rights to the RM Manage tool itself. No other RM tools can be accessed with this account.
Confirm Administrator Password	Re-enter the administrator password.
Install instance tables	**Selected:** When creating a new instance, you will create an empty instance. **Cleared:** During the creation process, the **Import** dialog opens from which you can import sample instances and backups.
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.

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 RM tables only**—Select the **Blank** instance from the **Sample Instances** tab.

- **Install a sample instance**—Select one of the sample instances (other than the Blank instance) from the **Sample Instances** tab:

| Instance	Description
BLANK	Use this instance to create an empty instance. This instance does not contain any classes. If you select the **Include Security Data** option, this will create the group **Administrators**, and the users **EPHOTO**, **EPHOTO_INFO**, **JOE** and **RTMADMIN**.
ALM_DEMO	This sample instance provides classes and data for pure software requirements management, creating ALM applications, including Test definition, planning, and execution. See chapter "Forms" on page 122 for information on creating the required forms.
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.

Instance	Description
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!

- Always start with the BLANK instance or an instance of your own that was created from the BLANK instance and then saved (see the Saved Instances tab).

- Do NOT use any sample instance other than BLANK as a starting point for an actual production instance.

- **Install a saved instance**—Select the instance from the **Saved Instances** tab.
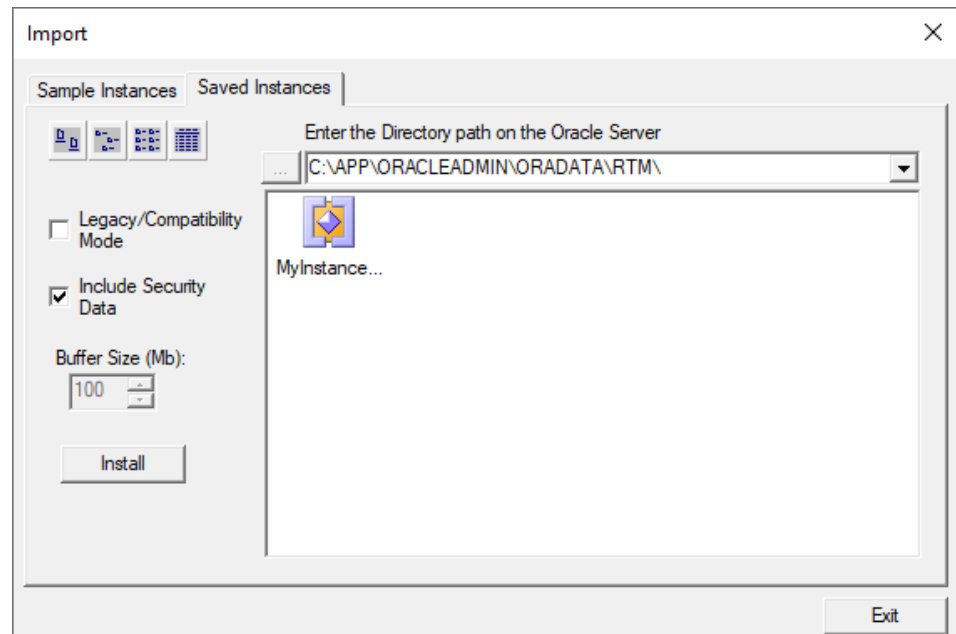
NOTE In Non-Legacy mode, you can only access backups that have been created with RM Manage. Backups copied to the server manually will not be available for selection.

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 .

10 Set the import options as needed:

Import Dialog	
Field	**Description**
Legacy/Compatibility Mode	**NOTE** 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	**NOTE** Legacy Mode and Sample Instances tab only. This sets the temporary space available for the operation.

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 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.

13 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.
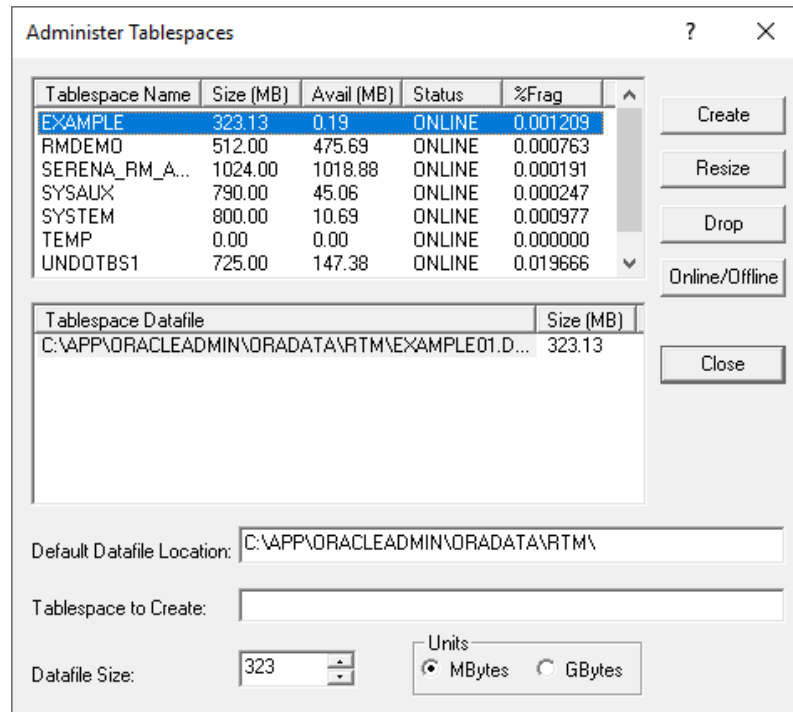
NOTE Administer Tablespace is not available in Amazon Cloud mode. For further information, see chapter "Using RM Manage within the Amazon Cloud" on page 280.

14 Select a datafile size and click **Resize**. A prompt asks "Do you wish to resize an existing datafile?".

15 Click **Yes**.

16 Click **Close**.

Advanced Options for 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.

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 236).

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.
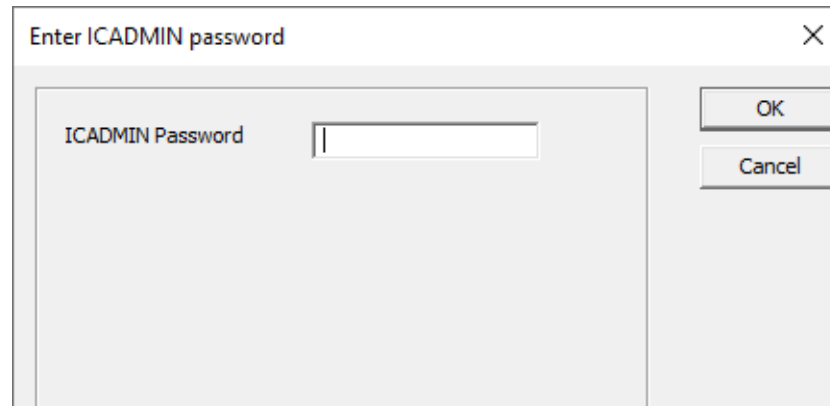

> **IMPORTANT!**
>
> ■   You must ensure that you create the ICDBA account (as explained in "Creating the ICDBA Account" on page 154) and associated password before assigning the password to ICADMIN. There is no software check to ensure that this has been done in the correct order.
>
> ■   When creating 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.
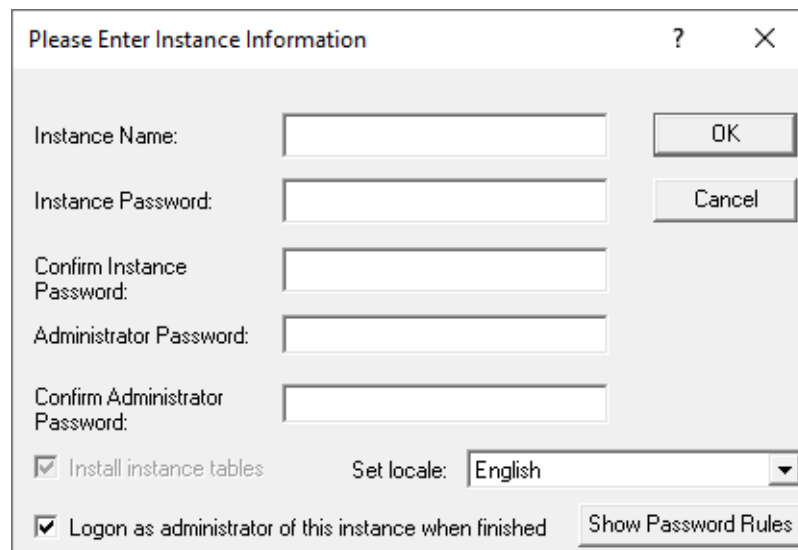
Execute the following steps in this dialog:

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).
	CAUTION! The instance name must follow the conventions specified in chapter "Naming Conventions for Instances" on page 30.
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.
	NOTE Instance passwords cannot begin with a number. For example, 12345 causes an error; however, a12345 is accepted. Click **Show Password Rules** for a summary of the rules.
Confirm Instance Password	Re-enter the instance password.
Administrator Password	Enter a password for the instance's administrator account. You will need this password to administrate the instance.
	NOTE The ID for this account is the instance name with Admin appended to the end, for example MyinstanceAdmin. Starting with RM 11.2.1, this account only has access rights to the RM Manage tool itself. No other RM tools can be accessed with this account.
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.
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.

> **IMPORTANT!**
>
> ■ You must ensure that you create the ICDBA account (as explained in "Creating the ICDBA Account" on page 154) 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.
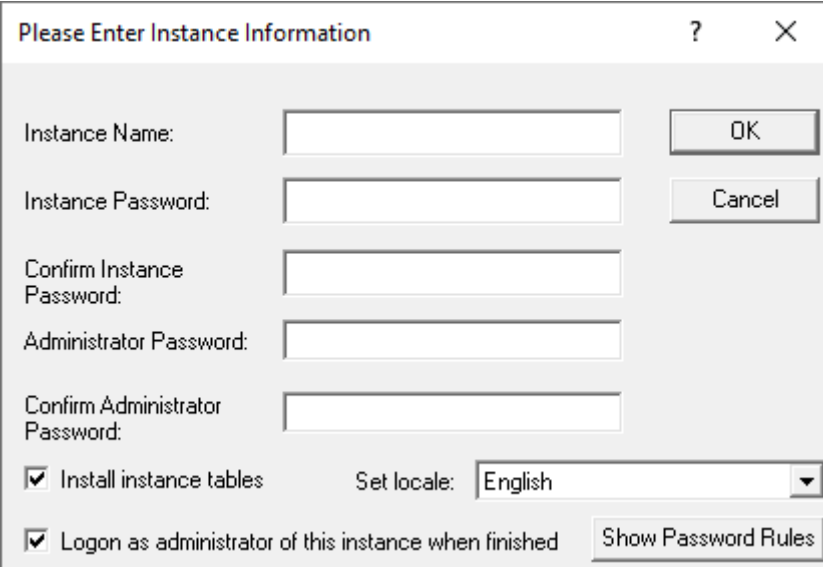
Execute the following steps in this dialog:

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.
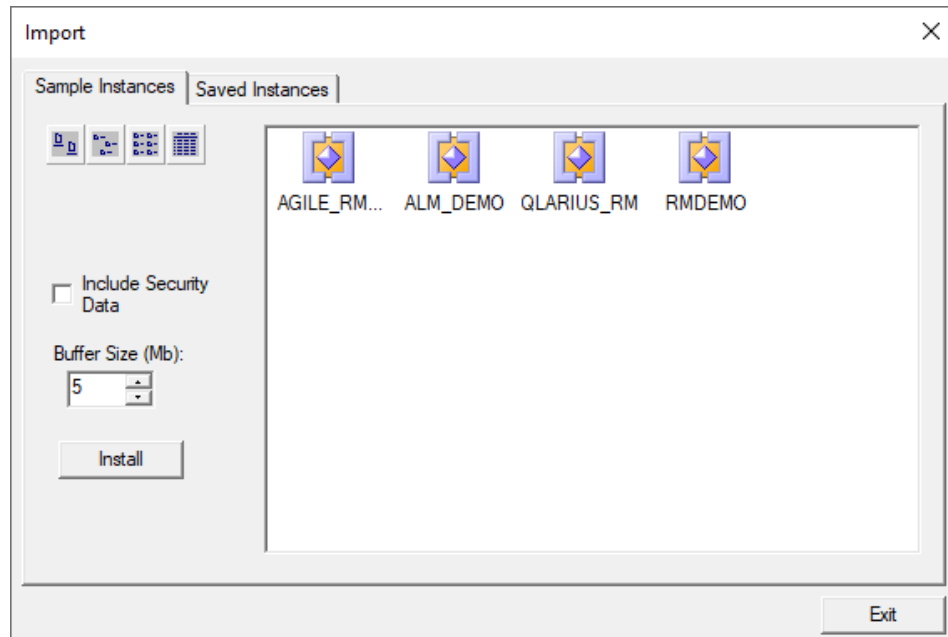
Please Enter Instance Information Dialog	
Field	**Description**
Instance Name ⚠️	Enter an instance name (for example, MYINSTANCE). **CAUTION!** The instance name must follow the conventions specified in chapter "Naming Conventions for Instances" on page 30.
Instance Password	Enter an instance password (for example, MYINSTANCE). This password is used by Dimensions RM to access Oracle. RM users do not use it directly in Dimensions RM. **NOTE** Instance passwords cannot begin with a number. For example, 12345 causes an error; however, a12345 is accepted. Click **Show Password Rules** for a summary of the rules.
Confirm Instance Password	Re-enter the instance password.
Administrator Password	Enter a password for the instance's administrator account. You will need this password to administrate the instance. **NOTE** The ID for this account is the instance name with Admin appended to the end, for example MyinstanceAdmin. This account only has access rights to the RM Manage tool itself. No other RM tools can be accessed with this account.
Confirm Administrator Password	Re-enter the administrator password.
Install instance tables	**Selected:** When creating a new instance, you will create an empty instance. **Cleared:** During the creation process, the **Import** dialog opens from which you can import sample instances and backups.
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.

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 (other than the Blank instance) from the **Sample Instances** tab:

Instance	Description
ALM_DEMO	This sample instance provides classes and data for pure software requirements management, creating ALM applications, including Test definition, planning, and execution. See chapter "Forms" on page 122 for information on creating the required forms.
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
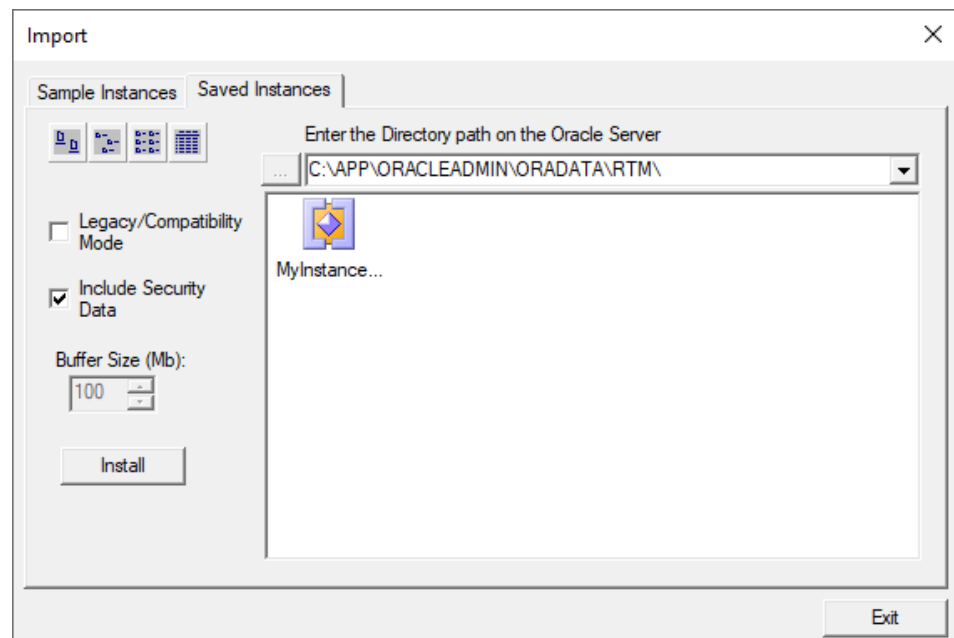
- Instances displayed with an instance icon contain data. Instances displayed with a class icon contain only the instance schema.
- To view the modification date and size of the files, click the Details button .

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 looking at 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 174. See also "Database Administrator Accounts: Changing Passwords and Unlocking" on page 222 and "Changing an Instance Administrator Password" on page 228.

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 174. See also "Database Administrator Accounts: Changing Passwords and Unlocking" on page 222 and "Changing an Instance Administrator Password" on page 228.

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 ![icon] , 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**.

Backing Up an Instance Account

Backup 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:

•   Micro Focus Common Tomcat

•   Micro Focus Dimensions RM Pool Manager

•   Micro Focus Dimensions RM E-Mail Notification Service

Note that stopping Micro Focus Common Tomcat will also disable other applications using this service.
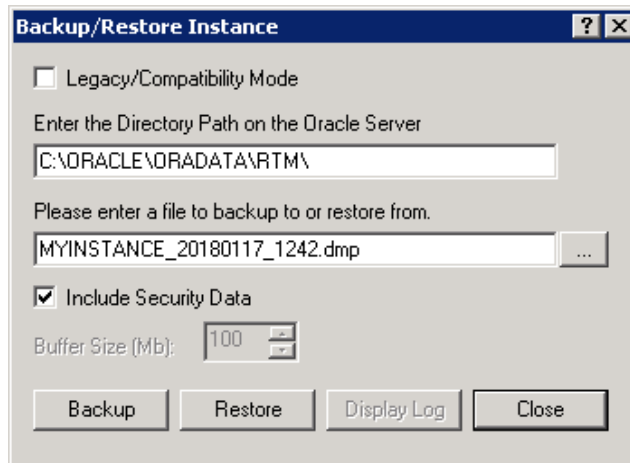
NOTE When running in Amazon Cloud mode, backups can only be created in legacy mode. For further information, see chapter .

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 .

3 Stop the **Micro Focus Dimensions RM E-Mail Service** service. This can be done from the following locations:

- RM Mail **Control** tab (see "Control Tab" on page 258)

- Windows **Services** (from the Windows **Control Panel**, double-click **Administrative Tools** and then double-click **Services**).

4 In **RM Manage**, select the instance you want to back up.

5 Select **File** | **Backup/Restore Instance Account**.

6 If prompted, enter your administrator password and click **OK**.

7 The Backup/Restore Instance dialog appears. Complete the following fields as needed.

Backup/Restore Instance Dialog	
Field	**Description**
Legacy/Compatibility Mode	Formats the backup so that can be imported on systems that only support legacy mode.
Oracle Directory Path	This field is automatically populated with the last modified server directory path for the selected instance. Edit the path as needed. **NOTE** This field is not available in Legacy Mode.
File Name	This field is automatically populated with a name for the backup file. The name is based upon the instance name and the current date and time. Edit this name as needed. **NOTE** ■ **Normal Mode:** The location is relative to the Oracle directory path. ■ **Legacy Mode:** The path to the Saved Projects directory of the RM installation is prepended to the file name.

Backup/Restore Instance Dialog	
Field	**Description**
...	Opens a dialog to select the backup file. **NOTE** **Normal Mode:** Enter the dump file name as described for the **File Name** field. **Legacy Mode:** This opens a file selection dialog to choose a file name for saving to backup.
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.
Buffer Size	**NOTE** Legacy Mode only. This sets the temporary space available for the operation. The default, and maximum, buffer size is 100MB. You can adjust the amount if needed.

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

9   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

10   Restart the **Micro Focus Dimensions RM E-Mail Service** service.

11   Restart the following services:

- Micro Focus Dimensions RM Pool Manager

- Micro Focus Common Tomcat

- Micro Focus 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:

- Micro Focus Common Tomcat

- Micro Focus Dimensions RM Pool Manager

- Micro Focus Dimensions RM E-Mail Notification Service

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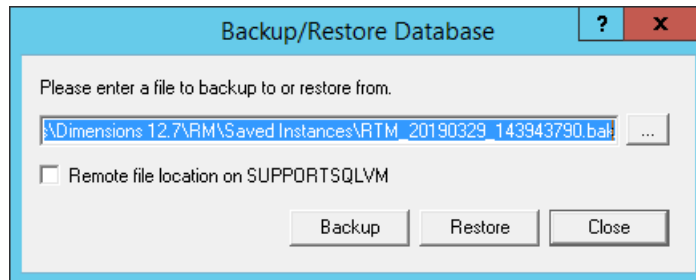
NOTE

- 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 280.

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 197.

3 Stop the **Micro Focus Dimensions RM E-Mail Service** service. This can be done from the following locations:

- RM Mail **Control** tab (see "Control Tab" on page 258)

- Windows **Services** (from the Windows **Control Panel**, double-click **Administrative Tools** and then double-click **Services**).

4 In **RM Manage**, right-click the database you want to back up and select **Backup/Restore Database** from the shortcut menu.

5 If prompted, enter the ICDBA 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	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.
	■ **Local mode:** The path to the Saved Instances directory of the RM installation is prepended to the file name.
	■ **Remote mode:** The location is relative to the MS SQL Server directory path.
	NOTE You can manually enter the name of the BAK file.
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 **Remote file location** 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 **Micro Focus Dimensions RM E-Mail Service** service.

10   Restart the following services:

- Micro Focus Dimensions RM Pool Manager

- Micro Focus Common Tomcat

- Micro Focus 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:
>
> - Micro Focus Common Tomcat
>
> - Micro Focus Dimensions RM Pool Manager
>
> - Micro Focus Dimensions RM E-Mail Notification Service
>
> Note that stopping Micro Focus Common Tomcat will also disable other applications using this service.
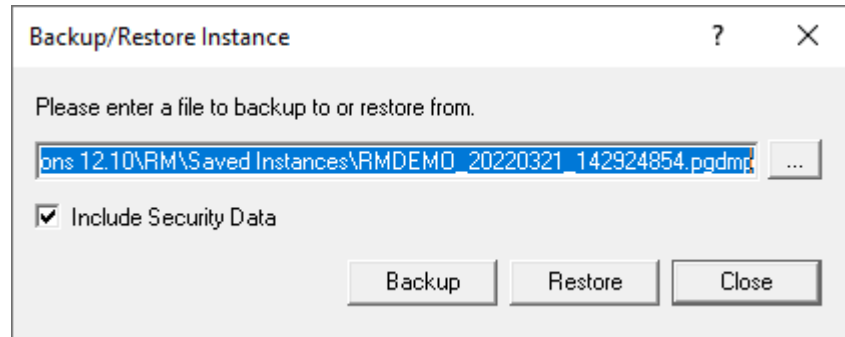
> **NOTE** The backup will always be created on the database server.

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 197.

3   Stop the **Micro Focus Dimensions RM E-Mail Service** service. This can be done from the following locations:

- RM Mail **Control** tab (see "Control Tab" on page 258)

- Windows **Services** (from the Windows **Control Panel**, double-click **Administrative Tools** and then double-click **Services**).

4   In **RM Manage**, select the instance you want to back up.

5   Select **File** | **Backup/Restore Instance Account**.

6   If prompted, enter your administrator password and click **OK**.

7   The Backup/Restore Instance dialog appears. Complete the following fields as needed.

Backup/Restore Instance Dialog	
Field	**Description**
File Name	This field is automatically populated with a name for the backup file. The name is based upon the database name and the current date and time. Edit this name as needed. ■ **Local mode:** The path to the Saved Instances directory of the RM installation is prepended to the file name. ■ **Remote mode:** The location is relative to the MS SQL Server directory path. **NOTE** You can manually enter the name of the BAK file.
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 **Remote file location** option is turned off.

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

9   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

10   Restart the **Micro Focus Dimensions RM E-Mail Service** service.

11   Restart the following services:

   • Micro Focus Dimensions RM Pool Manager

   • Micro Focus Common Tomcat

- Micro Focus 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:

- Micro Focus Common Tomcat

- Micro Focus Dimensions RM Pool Manager

- Micro Focus Dimensions RM E-Mail Notification Service

Note that stopping Micro Focus Common Tomcat will also disable other applications using this service.
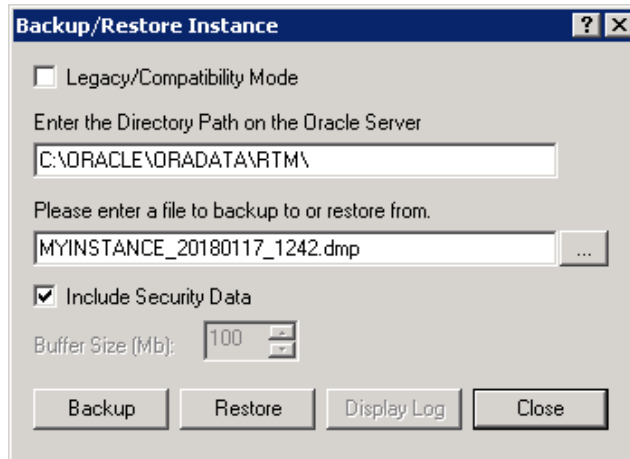
NOTE When running in Amazon Cloud mode, backups can only be restored in legacy mode. For further information, see chapter "Using RM Manage within the Amazon Cloud" on page 280.

To restore an instance account from a backup using the RM Manage interface:

1 Stop the **Micro Focus Dimensions RM E-Mail Service** service. This can be done from the following locations:

- RM Mail **Control** tab (see "Control Tab" on page 258)

- Windows **Services** (from the Windows **Control Panel**, double-click **Administrative Tools** and then double-click **Services**).

2 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 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 194.

3 In **RM Manage**, select the instance you want to restore.

4 Select **File | Backup/Restore Instance Account**.

5   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. **NOTE** This field is not available in Legacy Mode.
File Name	Enter the name of the file to restore from, or click **...** to select one. ■ **Normal Mode:** The file location is relative to the Oracle directory path. **NOTE** You can manually enter the name of the DMP file instead of selecting from those of the dialog. ■ **Legacy Mode:** The path to the Saved Projects directory of the RM installation is prepended to the file name.
...	Opens a dialog to select the backup file. ■ **Normal Mode:** The dialog contains the DMP file names available on the server. **NOTE** You can only see the DMP files that were made from the currently selected instance. ■ **Legacy Mode:** Opens a file selection dialog to choose the backup to restore. You can choose backup files from any available location.

Backup/Restore Instance Dialog	
Field	**Description**
Security Data	Imports all the users in the backed-up instance, as well as their permissions.
Buffer Size	**NOTE** Legacy Mode only. This sets the temporary space available for the operation. The default, and maximum, buffer size is 100MB. You can adjust the amount if needed.

6   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 237.

7   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

8   Restart the following services:

•   Micro Focus Dimensions RM Pool Manager

•   Micro Focus Common Tomcat

•   Micro Focus 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:

- Micro Focus Common Tomcat

- Micro Focus Dimensions RM Pool Manager

- Micro Focus Dimensions RM E-Mail Notification Service

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

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 280.

To restore an instance account from a backup using the RM Manage interface:

1 Stop the **Micro Focus Dimensions RM E-Mail Service** service. This can be done from the following locations:

   - RM Mail **Control** tab (see "Control Tab" on page 258)

   - Windows **Services** (from the Windows **Control Panel**, double-click **Administrative Tools** and then double-click **Services**).

2 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.

3 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	Enter the name of the file to restore from, or click **...** to select one. ■ **Local mode:** The path to the Saved Instances directory of the RM installation is prepended to the file name. ■ **Remote mode:** 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. **NOTE** You can manually enter the name of the BAK file.
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 **Remote file location** option is turned off.

4 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:

    a Enter the password for the ICADMIN user into the **ICADMIN Password** box.

    b Click **OK**.

5 Verify that the restore of the database completed without errors.

6 Restart the following services:

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

- Micro Focus 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:

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

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

To restore an instance account from a backup using the RM Manage interface:

1   Stop the **Micro Focus Dimensions RM E-Mail Service** service. This can be done from the following locations:

- RM Mail **Control** tab (see "Control Tab" on page 258)
- Windows **Services** (from the Windows **Control Panel**, double-click **Administrative Tools** and then double-click **Services**).

2   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 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 194.

3   In **RM Manage**, select the instance you want to restore.

4   Select **File | Backup/Restore Instance Account**.

5 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.
	▪ **Normal Mode:** The file location is relative to the Oracle directory path.
	NOTE You can manually enter the name of the DMP file instead of selecting from those of the dialog.
	▪ **Legacy Mode:** The path to the Saved Projects directory of the RM installation is prepended to the file name.
...	Opens a dialog to select the backup file.
	▪ **Normal Mode:** The dialog contains the DMP file names available on the server.
	NOTE You can only see the DMP files that were made from the currently selected instance.
	▪ **Legacy Mode:** Opens a file selection dialog to choose the backup to restore. You can choose backup files from any available location.
Include Security Data	Imports all the users in the backed-up instance, as well as their permissions.

6 Click **Restore**. The restore operation runs.

7 Click **Display Log** to view a log of the backup operation.

8 Restart the following services:

• Micro Focus Dimensions RM Pool Manager

• Micro Focus Common Tomcat

• Micro Focus 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, *not* the Dimensions RM user account password.
`-buffer` (optional)	**Valid values: 1…100** 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`	**Valid values: yes**, **no** **Yes** creates a backup file using the legacy format. **No** uses the newer format. **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 280.
`-rmdbausername`	**Valid value: ICDBA** The Oracle user ID for icmanage.
`-rmdbapassword`	The password of the Oracle user ID for icmanage.
`-encrypt`	**Valid values: yes**, **no** Specify **Yes** when using encrypted passwords. Specify **No** or do not use the `-encrypt` option when using passwords which are not encrypted.

Chapter 8 RM Manage

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 280.

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 -rmdbausername ICDBA
-rmdbapassword 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
-rmdbapassword <encrypted_ICDBAPassword>
-encrypt yes
```

To learn how to get encrypted passwords, see chapter "Backing up with Encrypted Password" on page 192.

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 -rmdbausername ICDBA
-rmdbapassword 9674BA5269718A05 -encrypt yes
```

190   Dimensions RM 12.10

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 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 190).

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 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 yes -rmdbausername ICDBA
-rmdbapassword 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 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 192.

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 yes -rmdbausername ICDBA
-rmdbapassword 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 192.

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 SQL Server instance name is RTM.

```
icmanage -location RTM -dumpfile e:\backup\rminstancebackup
-rmdbapassword 9674BA5269718A05 -encrypt yes
```

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 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 rminstancebackup in the backup directory of the E drive. The PostgreSQL instance name is DRM.

```
icmanage -location DRM -project rminstance -password pwd -dumpfile
e:\backup\rminstancebackup -rmdbausername ICDBA -rmdbapassword ICDBA
```

When you execute this command, the backup file rminstancebackup<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 192.

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 PostgreSQL instance name is DRM.

```
icmanage -location DRM -project rminstance -password 8548FE01CD673210
-dumpfile e:\backup\rminstancebackup -rmdbausername ICDBA
-rmdbapassword 9674BA5269718A05 -encrypt yes
```

When you execute this command, the backup file rminstancebackup<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 287 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 280.

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 "Backing Up an Instance Account" on page 175, 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 export all the user accounts that have been assigned to this instance schema, as well as user permissions, so that this data can be imported into another instance. If you do not want to export the security data, 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 280.

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 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 you wish to restore the schema from.

5   By default, the **Include Security Data** option is selected. This will import all users and groups that have been assigned to this instance schema, as well as user permissions. If you do not want to import the security data, 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 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

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 276.

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.

6 On the **User Info** tab, do the following:

    a Type the general user information.

    b 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**
>
> ■ 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 276.

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 267).

■   A valid LDAP configuration must have been specified (see chapter "Specifying the LDAP Configuration" on page 268).

■   LDAP must have been specified as a login source (see chapter "Specifying Login Sources" on page 263).

■   LDAP attributes must match your LDAP environment (see section "Configuring LDAP Attributes to match the environment" on page 203).

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

| RM Attribute	Registry Value	Default LDAP Attribute
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.
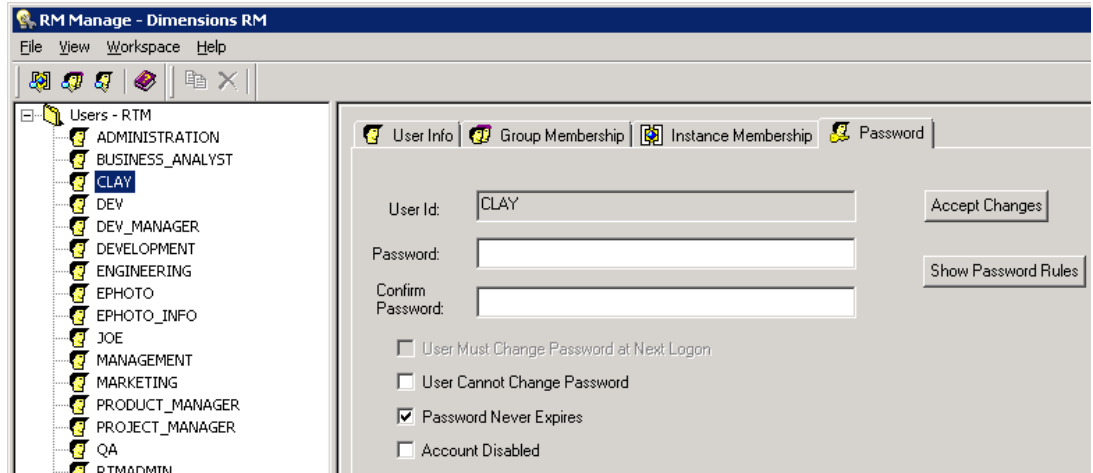
4   Enter new user password information.

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.
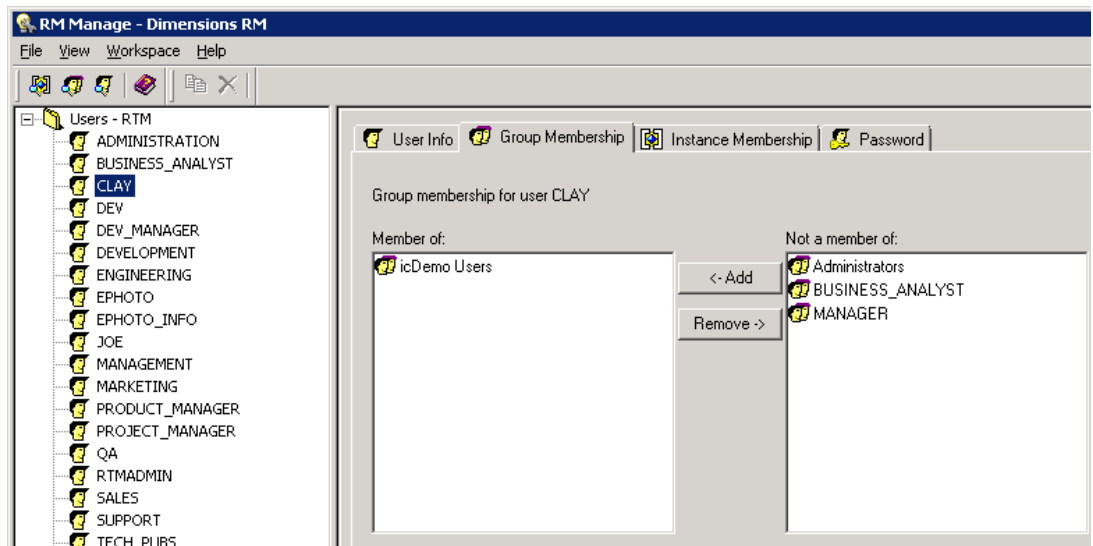
4   Select the groups to which you want to add the user from the list on the right.

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.
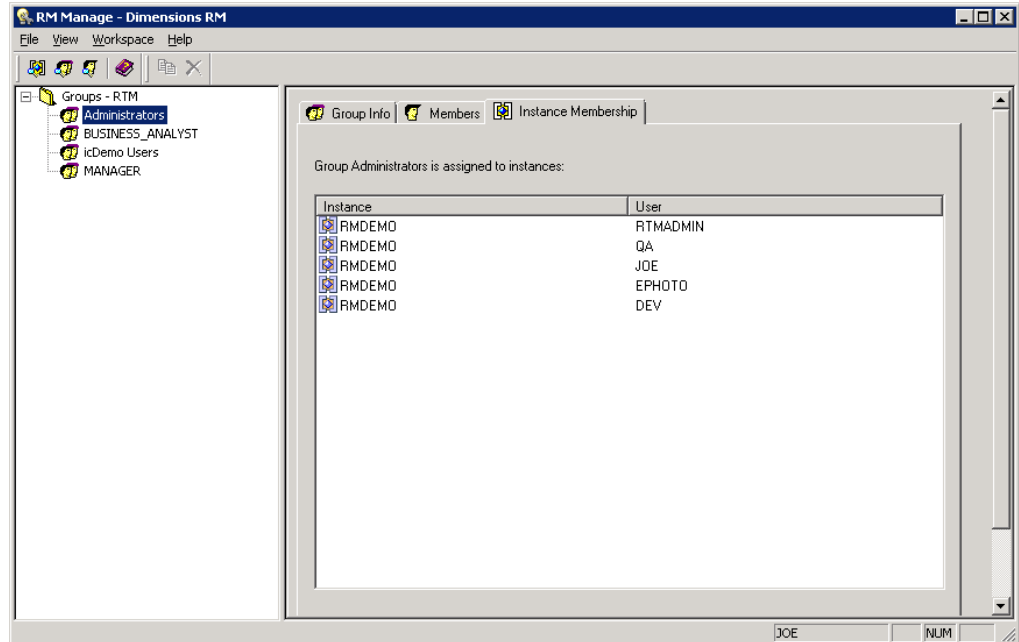
Administering Groups

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 - RM**).

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.
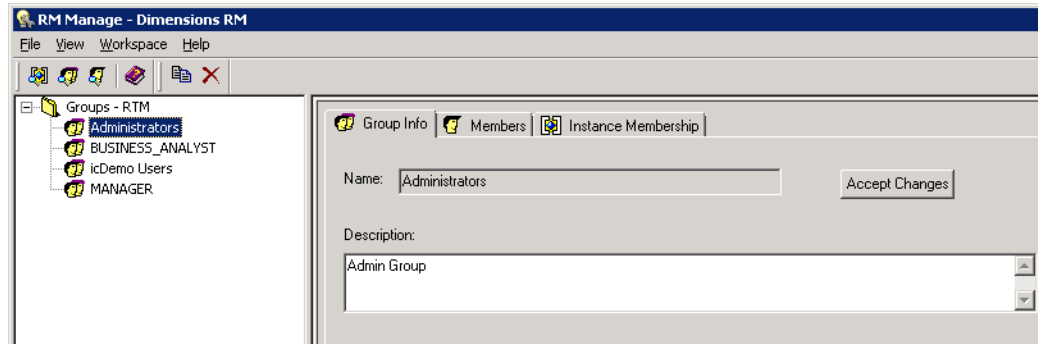
5   Click the **Group Info** tab and enter a user description.

6   Click **Accept Changes**.

> **NOTE** Creating a new group does not include it in public reports. If you wish that users of this group have access to public reports, you must allow this group access to each report.

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 - RM**).

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.
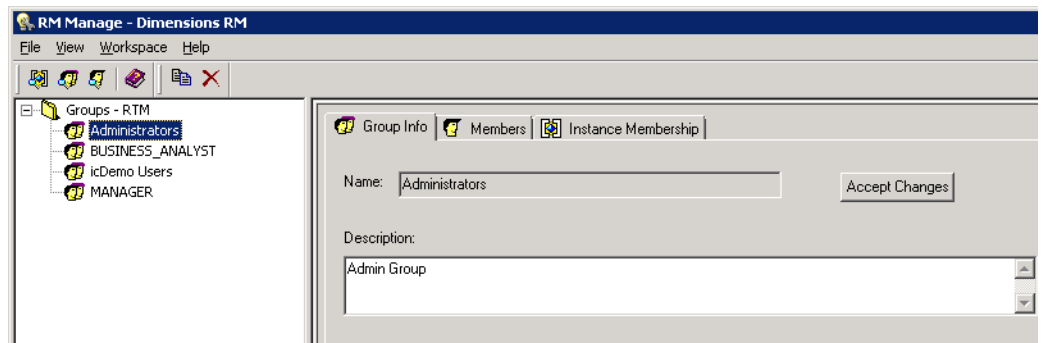
5   Click the **Group Info** tab and enter a user description.

6 Click **Accept Changes**.

> **NOTE**
>
> - Copying a group copies permissions (e.g. the "Create Class" right) and instance memberships from the source group. The assigned users of the source group are not copied.
>
> - Copying a group does not include it in public reports, even if the original group was allowed access to these reports. If you wish that users of the new group have access to public reports, you must allow this group access to each report.

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.
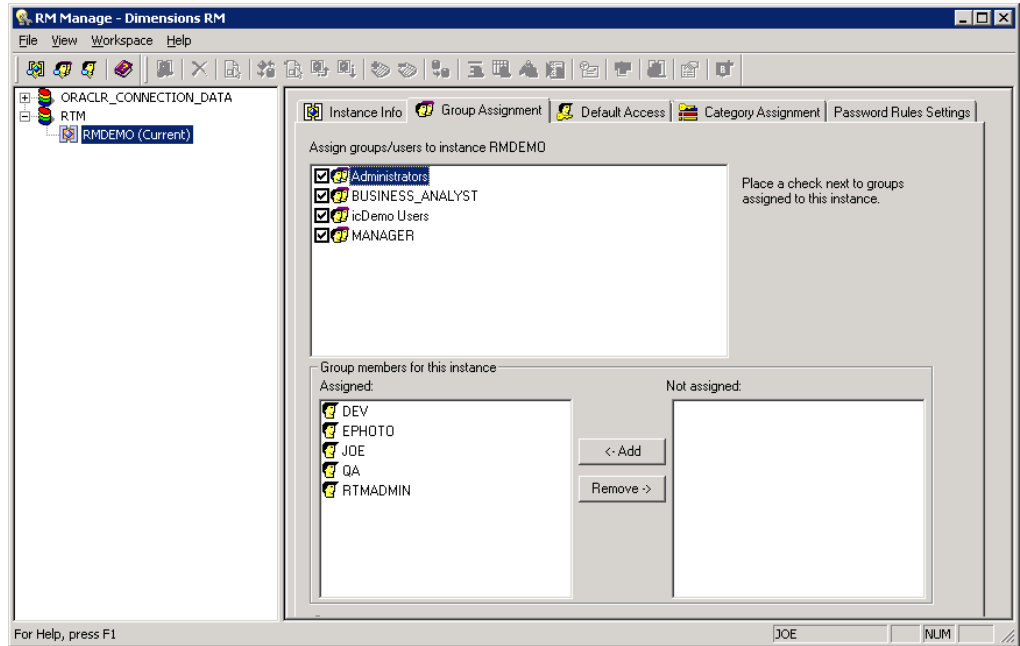
4   Select the group that contains the user you want to add to the instance. Selecting the check box automatically adds all members of that group to the instance. Clearing the check box automatically removes all members of that group from the instance.

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 205).

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

A resource is a data item such as a class, an attribute, or a document. A resource type represents a grouping of resources into a class of items. For example, a specific document falls into the type of "RMWord Documents." Each resource type has transactions that are appropriate for that type of resource. Transactions represent what can be done with that resource.

Showing or Hiding User Permissions

By default, RM Manage and Class Definition do not show user permissions. This is as having individual user permissions is much harder to maintain. Thus, it is strongly recommended to manage permissions through groups only.

NOTE

- If user permissions are defined, they will be used by Dimensions RM, even if user permissions are hidden.

- The user permissions feature is deprecated and will be removed in a later version.

To show or hide user permissions do the following:

1 Start RM Manage.

2 Select **Workspace | Options**. This opens the **Workspace Options** dialog.

3 Select the **Security** tab.

4 Do one of the following:

- **Show User Permissions:** Select the **Enable permissions for individual users (legacy mode)** box

- **Hide User Permissions:** Clear the **Enable permissions for individual users (legacy mode)** box

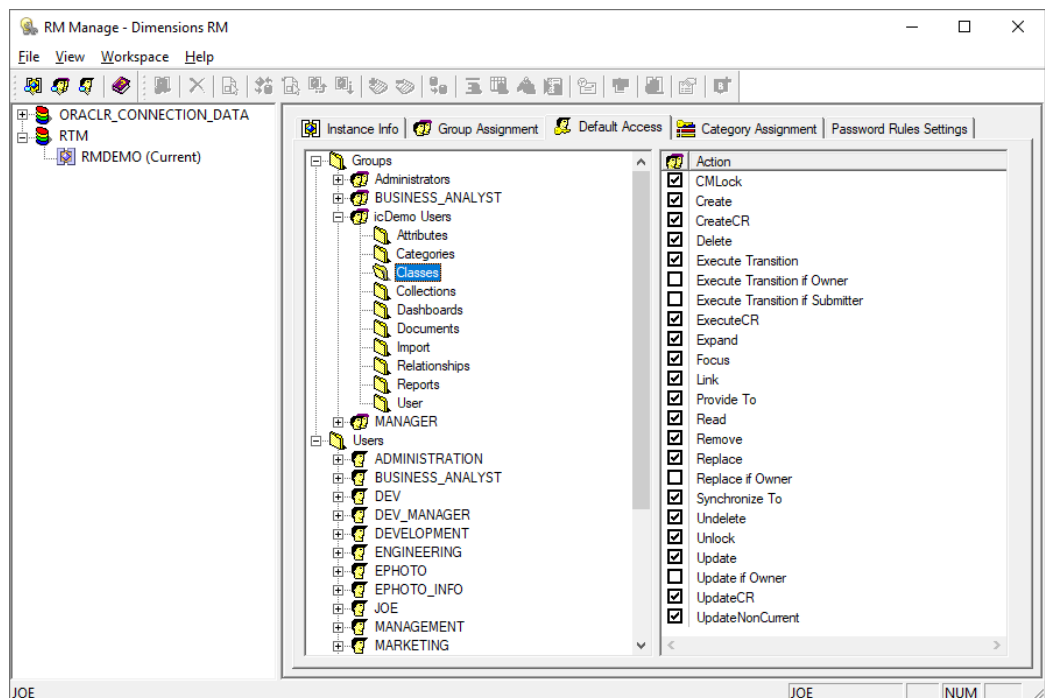**5** Click **OK**.

Setting Default Group Access

NOTES As a good general practice, Micro Focus recommends that no Dimensions RM group ever be granted the class access rights for: REMOVE, UPDATE, and UPDATE NON_CURRENT.

Update should not be granted to anyone on the system. All requirements changes should be performed with the replace function. This approach allows a fully auditable change history to be maintained and thus exposes Dimensions RM full capabilities. But this approach does require that you baseline requirements to capture the versions that you are currently capturing with the replace button. If users start using baselines and snapshots with other usage models (primarily updates and replace to version), they will be forced to create a new version just because someone else created a baseline. This may also limit the compare functions in Dimensions RM.

Default access rights may be set for a group. When you set default group access, all members of a group that do not have explicit access granted or denied (that is, they have inherited access) receive the access rights of their collective parent groups. The access rights that are granted are for types of entities, rather than for explicit instances of those entity types. The access rights that are granted here may be overridden for explicit instances. See "Security" on page 342 for details on overriding class definition default access.

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 the **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

By default, user permissions are hidden. For information on how to show user permissions, see chapter "Showing or Hiding User Permissions" on page 211.

NOTES As a good general practice, Micro Focus recommends that no Dimensions RM user (including Administrators) ever be granted the class access rights for: REMOVE, UPDATE, and UPDATE NON_CURRENT.

Update should not be granted to anyone on the system. All requirements changes should be performed with the replace function. This approach allows a fully auditable change history to be maintained and thus exposes Dimensions RM full capabilities. But this approach does require that you baseline requirements to capture the versions that you are currently capturing with the replace button. If users start using baselines and snapshots with other usage models (primarily updates and replace to version), they will be forced to create a new version just because someone else created a baseline. This may also limit the compare functions in Dimensions RM.

Please note that the user permissions feature is deprecated and will be removed in a later version.

Default access rights can be set for users. A user may be granted access, denied access, or may inherit the access rights of his or her parent groups. The access rights are for

types of entities, rather than for explicit instances of those entity types. The access rights may be overridden for explicit instances in other tools.
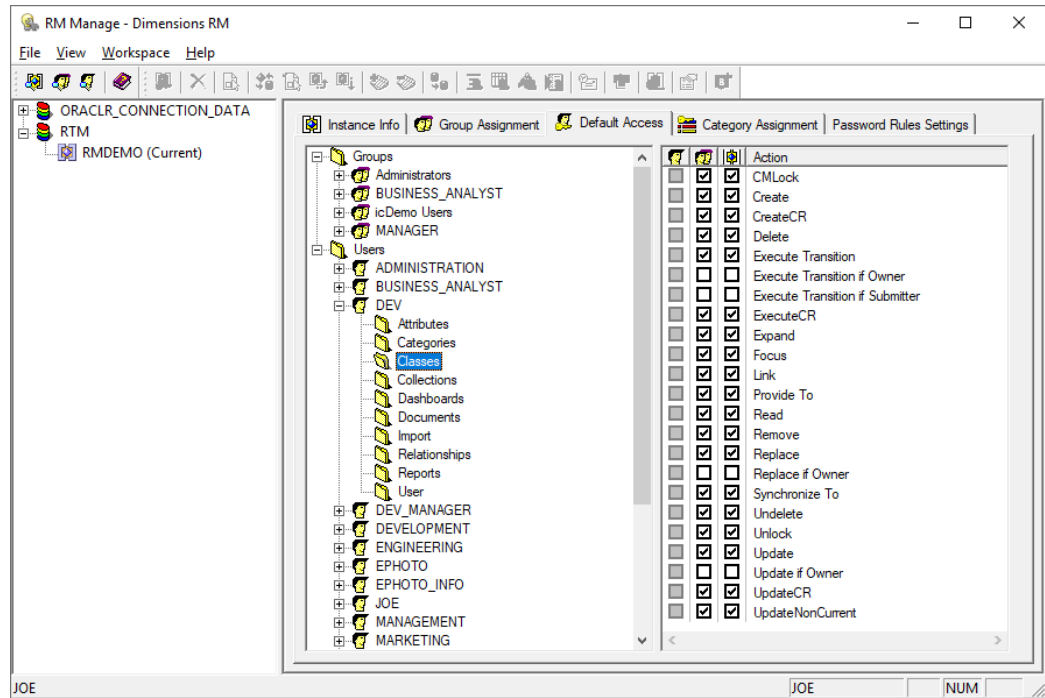
The group column in the right-hand list represents the access that has been set for the collective default access of the groups of which the user is a member. If the group column is checked (☑), the transaction has been granted for one or more of the groups. If the group column is not checked (☐), the group has not been given default access.

The user column in the right-hand list represents the access that has been set for the individual 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 from the group. The rows that are unchecked in the user column indicate that the user has been explicitly denied default access for this transaction. The rows that are checked in the user column indicate that the user has been explicitly granted default access for this transaction.

The instance column in the right-hand list indicates the net effect of the user and group default access for the instance. If this column is checked, the user has default access, either because it has been explicitly granted for the user or has been inherited from his or her groups. If this column is not checked, the user does not have default access, either because it has been explicitly denied or because default access has not been granted for any groups and the access has been inherited.

Granting All

Granting All Access Rights to a Group:

Groups may be granted access rights to all transactions within a specific resource type or to all transactions within every type. A resource is a data item such as a class, an attribute, or a document. A resource type represents a grouping of resources into a class of items. For example, a specific document falls into the resource type "RMWord Documents." Each resource type has transactions that are appropriate for that type of

resource. Transactions represent what can be done with that resource. For example, scripts may be created, read, updated, renamed and removed.

> **NOTE Grant All** does not grant the following transactions:
>
> **Classes:**
>
> - Remove
>
> - Update
>
> - UpdateNonCurrent
>
> **Collections:**
>
> - Delete Baseline

To grant access rights for every transaction 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* you want to grant all access rights for and select **Grant All**. This sets all of the transactions in this resource type to be explicitly granted for this group.

To grant access rights for every transaction 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.

Granting All Access Rights to a User:

Users may be explicitly granted access rights to all transactions within a specific resource type or to all transactions within every resource type. A resource is a data item such as a class, an attribute, or a document. A resource type represents a grouping of resources into a class of items. For example, a specific document falls into the type "RMWord Documents". Each resource type has transactions that are appropriate for it. Transactions represent what can be done with that resource. For example, scripts may be created, read, updated, renamed, and removed.

To grant access rights for every transaction 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 **Users** folder.

5   Expand the user to see the types of resources that may be assigned default access.

6   Right-click the *resource type* you want to grant all access rights for and select **Grant All**. This sets all of the transactions in this resource type to be explicitly granted for this user.

To grant access rights for every transaction in every resource type:

1   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 **Users** folder.

5   Right-click the *user* to which you want to grant all access rights and select **Grant All**. This sets all of the transactions in every resource type to be explicitly granted for this user.

Revoking All

Groups may be denied access rights to all transactions within a specific resource type or to all transactions within every type. Users may be explicitly denied access rights to all transactions within a specific type or to all transactions within every type.

A resource is a data item such as a class, an attribute, or a document. A resource type represents a grouping of resources into a class of items. For example, a specific document falls into the type "RMWord Documents." Each resource type has transactions that are appropriate for that type of resource. Transactions represent what can be done with that resource. For example, scripts may be created, read, updated, renamed, and removed.

To revoke access rights for every transaction 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* for 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 transaction 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.

Inheriting All Access Rights for a User

Users can inherit access from their groups for all transactions within a specific resource type or all transactions within all resource types. A resource is a data item such as a class, an attribute, or a document. A resource type represents a grouping of resources into a class of items. For example, a specific document falls into the type "RMWord Documents." Each resource type has transactions that are appropriate for that type of resource. Transactions represent what can be done with that resource. For example, scripts may be created, read, updated, renamed and removed.

To grant access rights for every transaction 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 inherit default access.

3   Click the **Default Access** tab.

4   Click + to expand the **Users** folder.

5   Click + next to the relevant *user* to see the types of resources that may be assigned default access.

6   Right-click the *resource type* for which you want to inherit all access rights and select **Inherit All**. This sets all of the transactions in this resource type to be inherited for this user. The user does not have access rights explicitly granted or denied for any transaction in this resource type, but instead inherits his or her group access rights for these transactions.

7   When prompted, click **Yes** to confirm the inherit all action.

To grant access rights for every transaction 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 inherit default access.

3 Click the **Default Access** tab.

4 Click + to expand the **Users** folder.

5 Right-click the *user* for whom you want to inherit all access rights and select **Inherit All**. This sets all of the transactions in every resource type to be inherited for this user. The user does have access rights explicitly granted or denied for any transaction, but instead inherits his or her group access rights.

6 Click **Yes** to confirm the inherit 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 a user access, deny a user access, or allow a user to inherit the access rights of his or her 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.
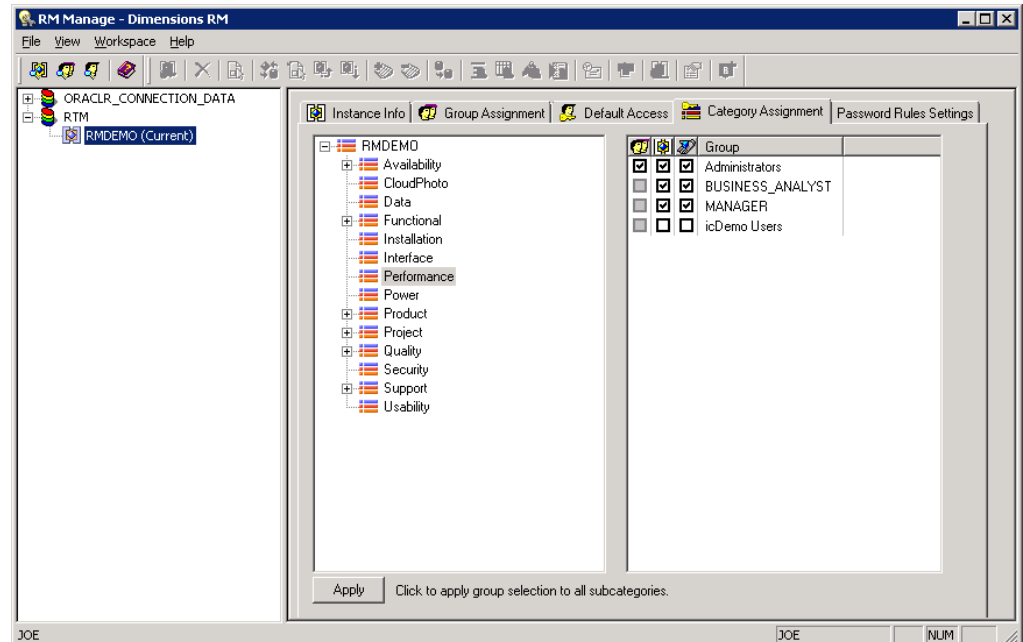
4 In the tree in the left pane, select the category to which you want to assign permissions.

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 276.

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

NOTES   As a good general practice, Micro Focus recommends that no Dimensions RM group or user (including Administrators) ever be granted the class access rights for: REMOVE, UPDATE, and UPDATE NON_CURRENT.

Update should not be granted to anyone on the system. All requirements changes should be performed with the replace function. This approach allows a fully auditable change history to be maintained and thus exposes Dimensions RM full capabilities. But this approach does require that you baseline requirements to capture the versions that you are currently capturing with the replace button. If users start using baselines and snapshots with other usage models (primarily updates and replace to version), they will be forced to create a new version just because someone else created a baseline. This may also limit the compare functions in Dimensions RM.

Group and user access rights are maintained within RM Manage. The administrator can assign default access to group and user accounts. For example, a user can be granted read-only privileges, but not be granted the ability to update data. In addition to granting specific privileges to users, the administrator can also allow a user to inherit rights from his or her groups. Users can be given access to more than one group and have different privileges for each. Therefore, a user can have specified privileges for different instances. The administrator can also grant or deny privileges at the group level.

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 287 and "Order of Precedence" on page 228 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.
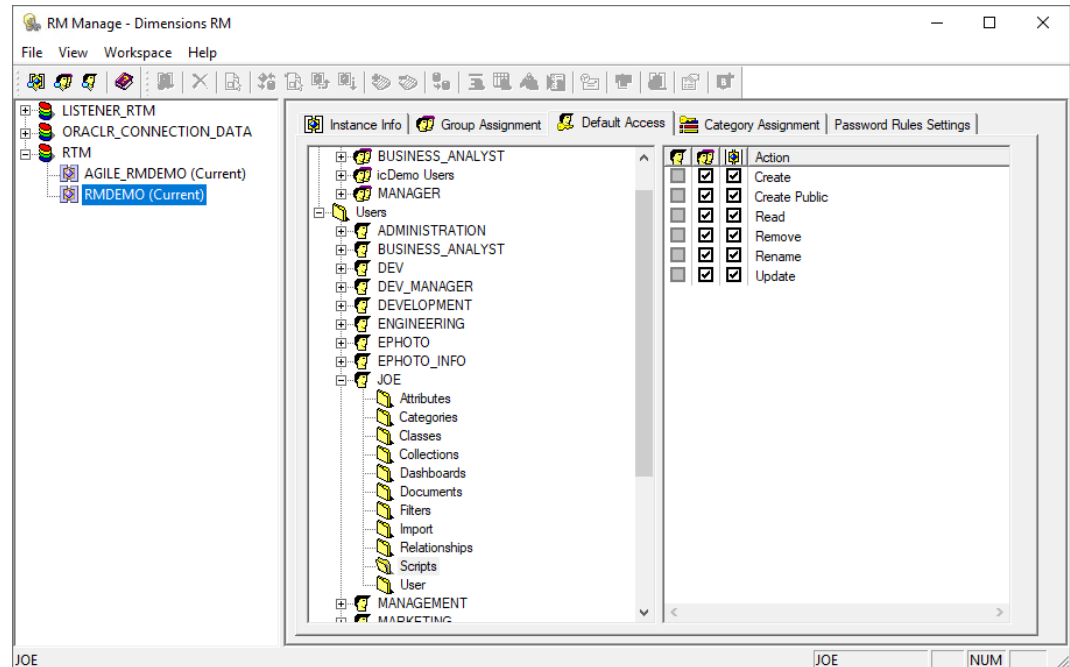
The user's default access for **Scripts** shows that the **Create** and **Read** transactions are not selected in the group column ⚇. Those transactions have not been granted for the groups to which the user belongs. The user column ⚇ represents the access that has been set for the user. The rows that 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 174, "Updating the Instance Password" on page 174, and "Changing an Instance Administrator Password" on page 228.

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: Changing Passwords and Unlocking" on page 222.
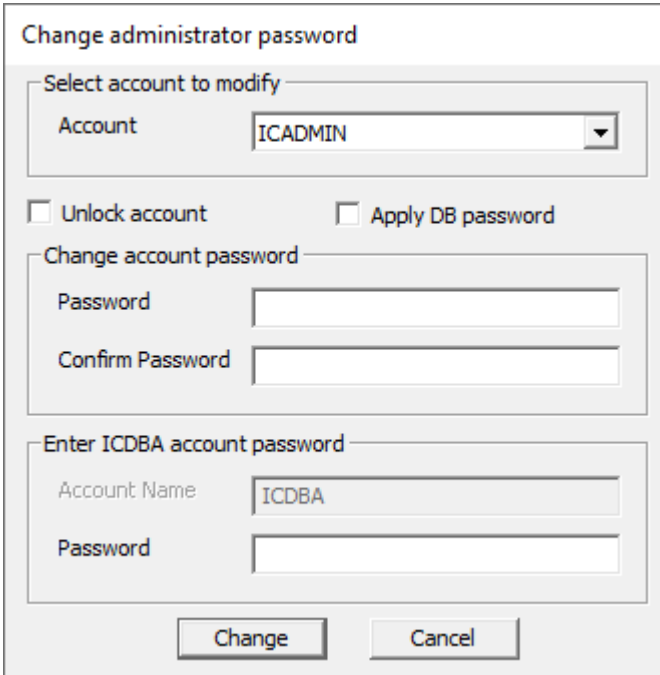
Unlocking the ICDBA Account

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.

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
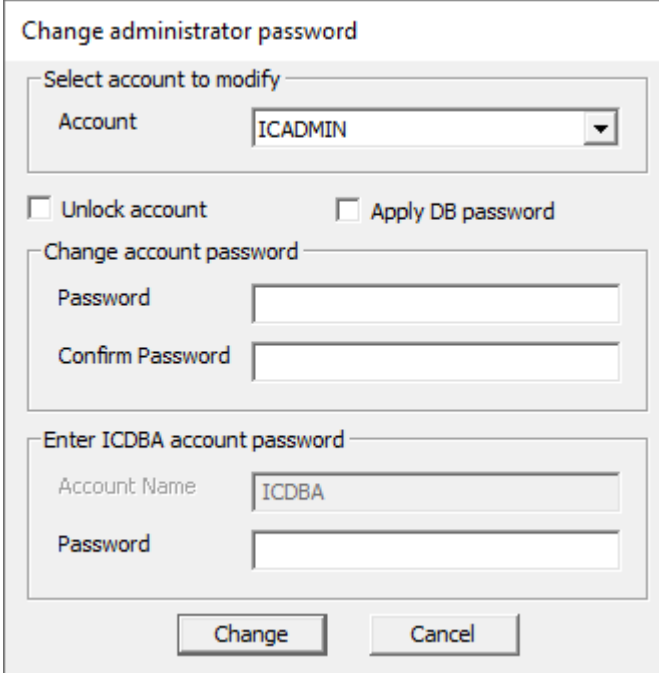
If the password of the ICADMIN account was changed in the database and not through RM Manage, please refer to chapter "Updating the ICADMIN Password in Security.dat" on page 225.

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: Changing Passwords and Unlocking" on page 222.

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 .

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: Changing Passwords and Unlocking" on page 222.

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.

```
Change administrator password
 ┌─Select account to modify ──────────────────────┐
 │  Account            [ICADMIN            ▼]       │
 └─────────────────────────────────────────────────┘

 ☑ Unlock account          ☐ Apply DB password
 ┌─Change account password ───────────────────────┐
 │  Password        [                        ]     │
 │  Confirm Password [                       ]     │
 └─────────────────────────────────────────────────┘

 ┌─Enter ICDBA account password ──────────────────┐
 │  Account Name     [ICDBA                 ]      │
 │  Password         [                      ]      │
 └─────────────────────────────────────────────────┘

            [ Unlock ]      [ 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 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 174 and "Database Administrator Accounts: Changing Passwords and Unlocking" on page 222.

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
Attribute Transactions	
Update	The user can change the attribute value.
Board Transactions	
Create Public	The user can create public boards and dashboards.
Category Transactions	
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 "Assigning Categories" on page 218. **NOTE:** 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.
Class Transactions	

Transaction	Definition
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."
Collection Transactions	
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.
Document Transactions	
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 **does not** 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.
Import Transactions	
Import	The user can import documents and requirements.
Relationship Transactions	
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.
Report Transactions	
Create	The user can create new reports. **NOTE:** 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.
User Transactions	
Team Maintenance	The user can create, edit, and delete Agile teams.
User Group Assignment	The user can assign users to groups.

Creating Category Administrators

When using categories as projects, you might want to allow people other than the administrator to manage certain functions, e.g. allow user access to that category aka project.

To make a user a category administrator, execute these steps:

1   Create a group which refers to the category, e.g. *CLOUDPHOTO_ADMIN* (see chapter "Creating a New Group" on page 207).

2   Change to the Default Access tab and select the Categories folder (see chapter "Default Access" on page 221).

3   Enable the rights **Category Assignment**, **Define List Values**, or **Maintain Sub-Categories**, depending on your needs (see chapter "Valid Transactions" on page 229).

4   If users are also assigned to different groups matching the category (e.g. *CLOUDPHOTO_USER*), you might also want to assign the **User Group Assignment** right (in the **User** folder).

5   Select the **Category Assignment** tab and assign the group to the desired category (see chapter "Assigning Categories" on page 218).

6   Assign one or several users to the category administrator group (e.g. *CLOUDPHOTO_ADMIN*), see chapter "Adding a User to a Group" on page 205.

7   Assign the users to the instance (see chapter "Assigning Users to Groups" on page 209).

Database Password Encryption

Database password encryption lets you control the password for the ICADMIN Oracle user account. This prevents unwanted personnel from connecting to the database to read and modify data.

To accomplish this, you use a file named security.dat that contains the password in an encrypted form. Dimensions RM uses the 3-DES encryption algorithm with three encryption keys. These encryption keys can be changed using the RM Manage **Change Encryption Keys** dialog box.

For the database concerned, the security.dat file contains :

- A database identifier (for example, [RM]).

- The three encryption keys.

- The encrypted password for ICADMIN.

To change the ICADMIN encryption keys:

1   In **RM Manage**, select the database whose ICADMIN encryption keys you want to change.

2   Select **File** | **Change Encryption Keys**, click the **Change Encryption Keys** button , or right-click the database and select **Change Encryption Keys**.

3   The **Change Encryption Keys** dialog box opens.
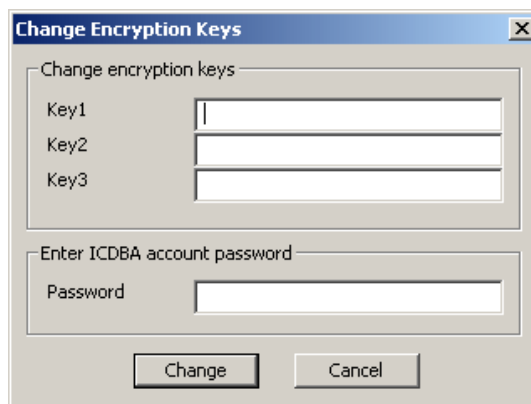
4   In the **Change encryption keys** area, type the new keys in the **Key1**, **Key2**, and **Key3** fields.

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

6   In the **Enter ICDBA account password** area, type the current ICDBA password.

7   Click **Change**.

Changing the Location of the security.dat File

The default security.dat file is automatically installed in top-level of the Dimensions RM installation directory (RTM_HOME). You can change the default location during installation

or move it to another location later. If you do so, each user must then use RM Manage to specify its location.

> **NOTE** If no `security.dat` file is found in the specified location, the default encrypted passwords are used. These are the same encrypted passwords that are in the default `security.dat` file that was installed.

For information about using RM Manage to specify the location of the `security.dat` file, see "Setting the Location of the Database Password File" on page 154.

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 "Backing Up an Instance Account" on page 175. 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.
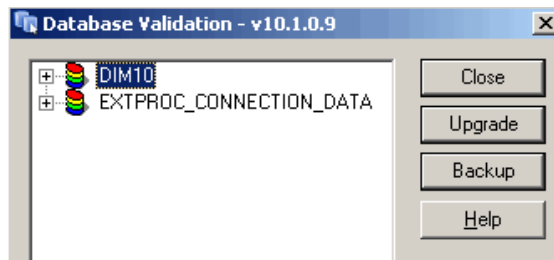
3   To expand the database that contains the instance you want to convert, click +.

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 326. 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.
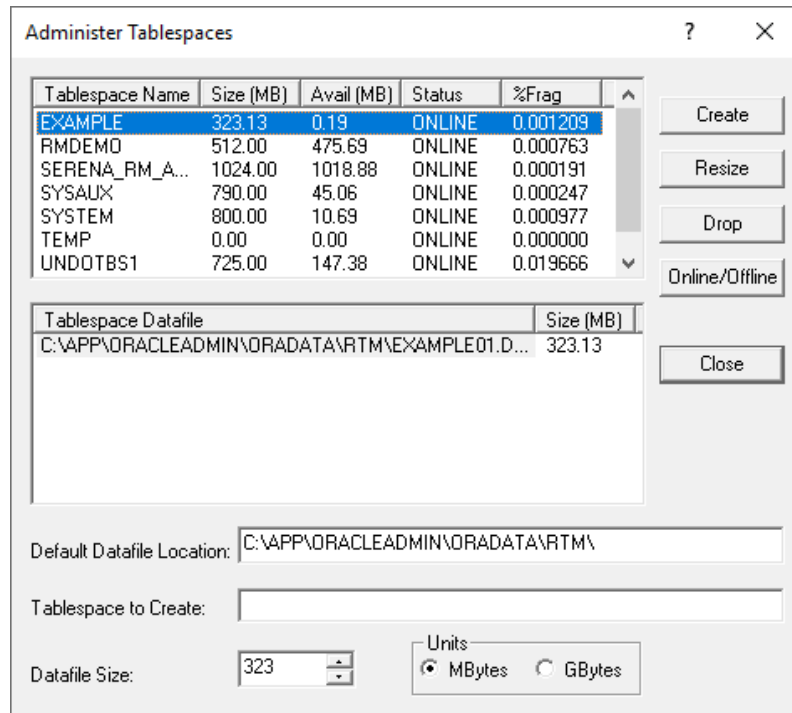
4   Enter a name in **Tablespace to Create** for the tablespace.

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.

Managing Locks

Dimensions RM classes, objects, collections, and source documents are implemented as sets of values within database tables. The set of values that defines a single object or collection is referred to as a *record*. When records are locked, they cannot be modified. RM Manage locks objects in use, such as documents opened by users. However, open records may remain locked after a system crash. Lock management is provided as a means of freeing records that have been locked as a result of a system crash.

It is also desirable to lock records temporarily to prevent others from changing the contents while some other action takes place. Lock management also provides a configuration management lock (CMLock), which is a way to lock records that should not be changed.

For security, only those records that are locked by the current user will be available to unlock; or, if the current user has been granted Unlock privileges, all of the user locked records will be available to unlock. Only users who have been granted CMLock privileges will be allowed to lock records for CM purposes. Only users who have been granted CMLock privileges will be allowed to unlock CM locked records.

> **NOTE** You cannot use CMLock to unlock objects that are baselined.

Locking Objects

Use CM Lock when you want to keep an object from being modified. CM Lock can be used only for objects.

To lock objects:

1   In **RM Manage**, select an instance.

2 Select **File | Administer Locks**, click the **Administer Locks** button 🖼, or right-click an instance and select **Administer Locks**. The **Lock Manager** dialog box opens.
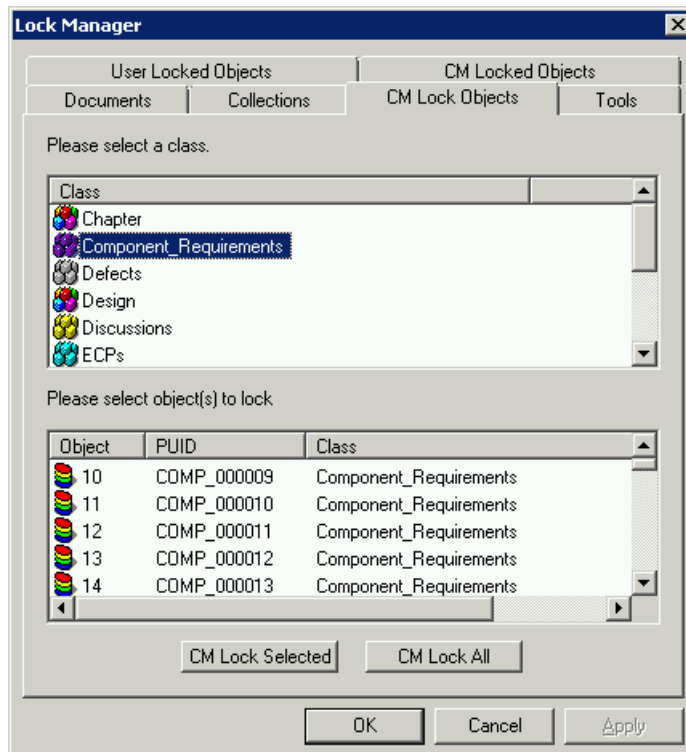
3 Click the **CM Lock Objects** tab.

4 Select a class from the class list.

5 Select the objects you want to lock from the object list.

6 Click **CM Lock Selected** to lock only the selected objects, or **CM Lock All** to lock all of the objects for the selected class.

Unlocking Collections

This function no longer exists.

Unlocking Documents

To unlock documents:

1 In **RM Manage**, select an instance.

2 Select **File | Administer Locks** or click the 🖼 button. The **Lock Manager** dialog box opens.

3 Click the **Documents** tab.

4 Select the locked documents you want to unlock from the list. Locked documents are indicated by a 🖼 icon.

5 Do one of the following:

■ Click **Unlock Selected** to unlock only the selected documents or **Unlock All** to unlock all of the locked documents.

■ Right-click and select **Unlock**.

Unlocking Objects

To unlock objects:

1 In **RM Manage**, select an instance.

2 Select **File | Administer Locks** or click the ![button] button. The **Lock Manager** dialog box opens.

3 Click the **CM Locked Objects** tab.
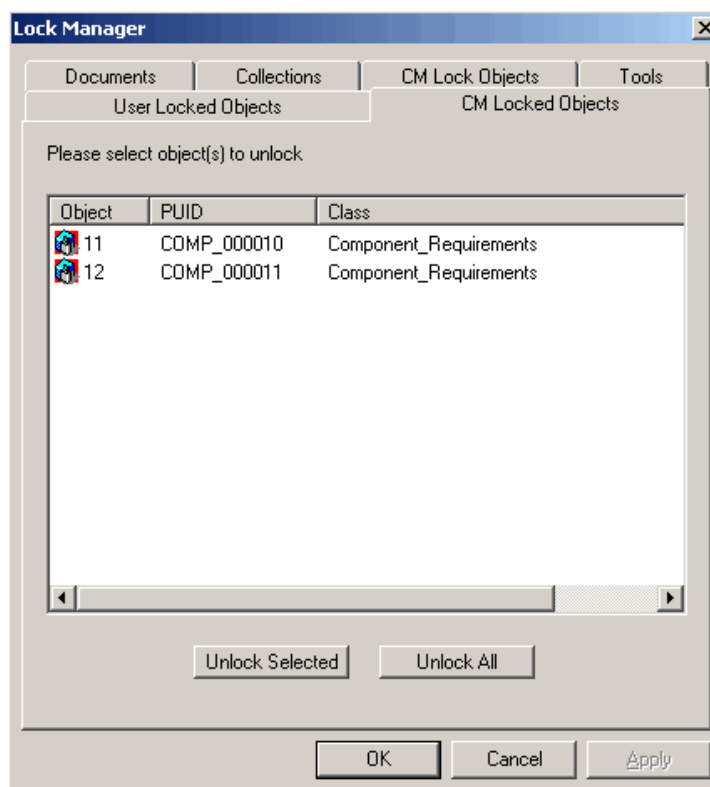
4 Select the locked objects you want to unlock from the list. Locked objects are indicated by an ![icon] icon.

5 Do one of the following:

■ Click **Unlock Selected** to unlock only the selected objects or **Unlock All** to unlock all of the locked objects.

■ Right-click and select **Unlock**.

Unlocking Tools

This function no longer exists.

E-mail Registration

The instance administrator can administer e-mail rules on a specific instance. This section contains information on configuring e-mail messages and rules, and creating, modifying, and deleting rules.

Configuring E-Mail Messages and Rules

You can configure the following items from the **E-Mail Registration** dialog box:

- **Classes**—Individual classes can be enabled and disabled, thereby providing a simple method of disabling all rules that have been defined for a specific class.

- **Display Attributes**—A list of attributes that should be included in all e-mails can be specified. Each user can defined their own set of attributes to be included in the e-mail that will be inserted after the administrator-defined attributes.

- **Message Text**—A paragraph of pre- and post-message text can be defined. The pre-message text will be inserted at the start of the e-mail message, and the post-message text will be inserted at the end.

- **Subject Text**—The subject line for the e-mail can be defined. Attribute values can be included in the subject line.

- **Users**—Rules for all users can be administered in a single place. Rules can be created, modified and deleted for any user.

Enabling and Disabling Classes

You can define which class or classes should be enabled for e-mail notification. The RM Mail service only processes rules for classes that have been enabled.

You typically want to temporarily disable e-mail notification for a class while performing a large update operation, such as a batch update. Disabling e-mail notification for a class does not delete the rules that have been defined for the class; it simply suppresses the processing of rules for the class.

To enable or disable e-mail notification for a class:

1   In **RM Manage**, right-click the instance, and select 🖼 **Administer Email**. The **E-Mail Registration** dialog box opens.

2 Select the **Classes** branch. A list of all classes for the instance is displayed in the right part of the dialog. Classes that are enabled have a checkmark in the check box next to them, while classes that are disabled have an empty check box next to them.
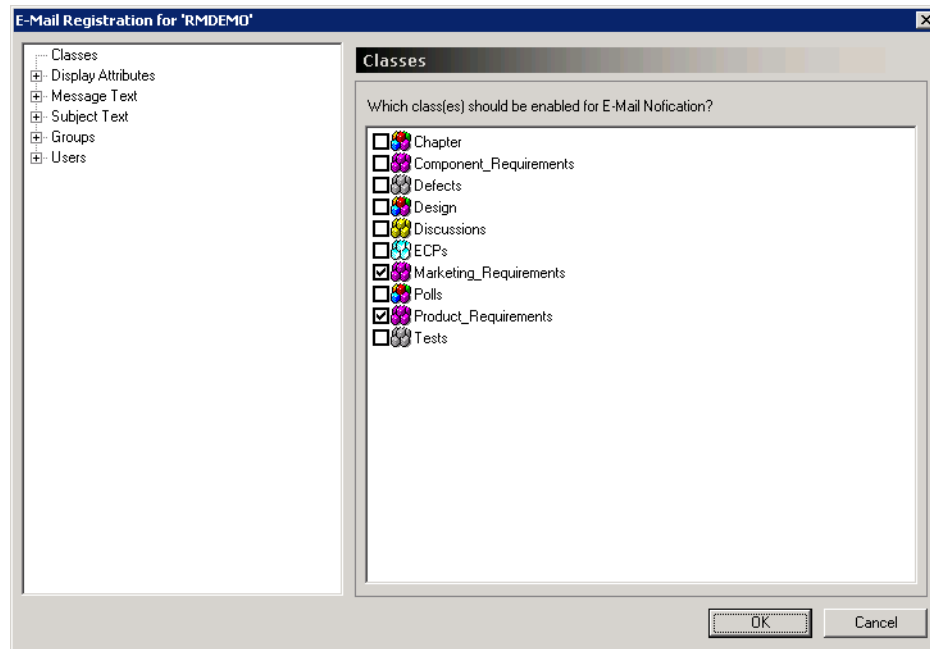
3 Select the check box to the left of the desired class to enable or disable e-mail notification for it.

4 If you disable notification for all classes, do the following after you disabled the last class:

   a Start the **RM Mail** configuration applet by selecting P**rograms | Micro Focus | Dimensions RM *version* | RM Mail Configuration** from the Windows **Start** menu.

   b Execute the steps described in chapter "Removing Unsent E-Mail Notifications from the Mailing Queue" on page 259.

Defining Display Attributes

You can define a list of attributes that should be included with all e-mails sent for a specific class.

You can include a default set of attributes for all classes that do not have a specific set of attributes defined. The values for the administrator-defined attributes will be included in the e-mail prior to the attributes that the user selects to display when creating a rule.

To define which attributes should be included:

1 In **RM Manage**, right-click the instance, and select **Administer Email**. The **E-Mail Registration** dialog box opens.

2 Expand the **Display Attributes** branch in the left-hand graphical tree and select the desired class.

On the right, two lists are displayed: the left list contains a list of attributes that will not be included with the e-mail, while the list on the right displays a list of attributes that will be included.
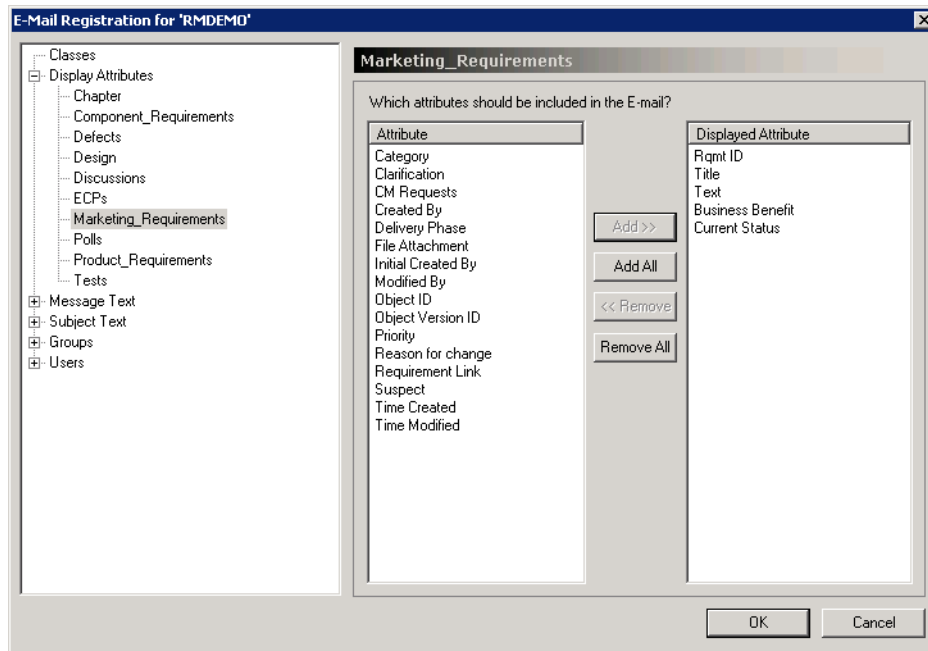
3   Select the attribute in either list and click **Add** or **Remove**.

To change the order of attributes:

▪   Drag-and-drop the attributes in the **Displayed Attribute** list to the desired order.

To define a default set of attributes:

1   Select the **Displayed Attributes** branch.
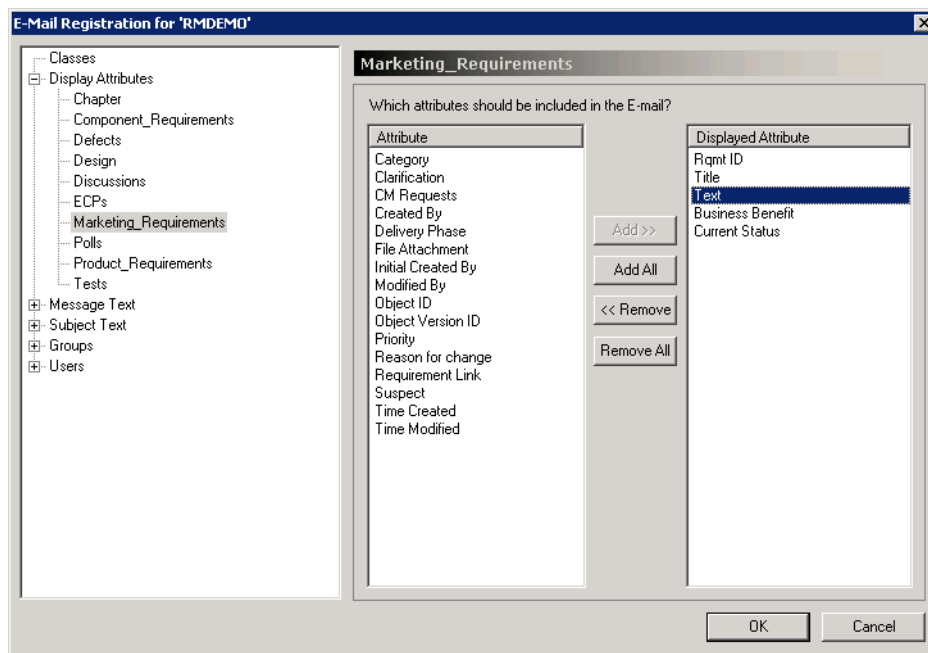
2   Add or remove attributes as described earlier in this section.

Defining Message Text

You can define a block of pre- and post-message text for each class. The pre- and post-message text is included with all e-mails generated by rules for the class. The pre-message text is included as the very first item in the e-mail while the post-message text will be included as the last item in the e-mail.

You can include a default pre- and post-message for all classes that do not have specific pre-message or post-message text defined.

To define pre-message and post-message text:

1　Expand the **Message Text** branch and select the appropriate class.
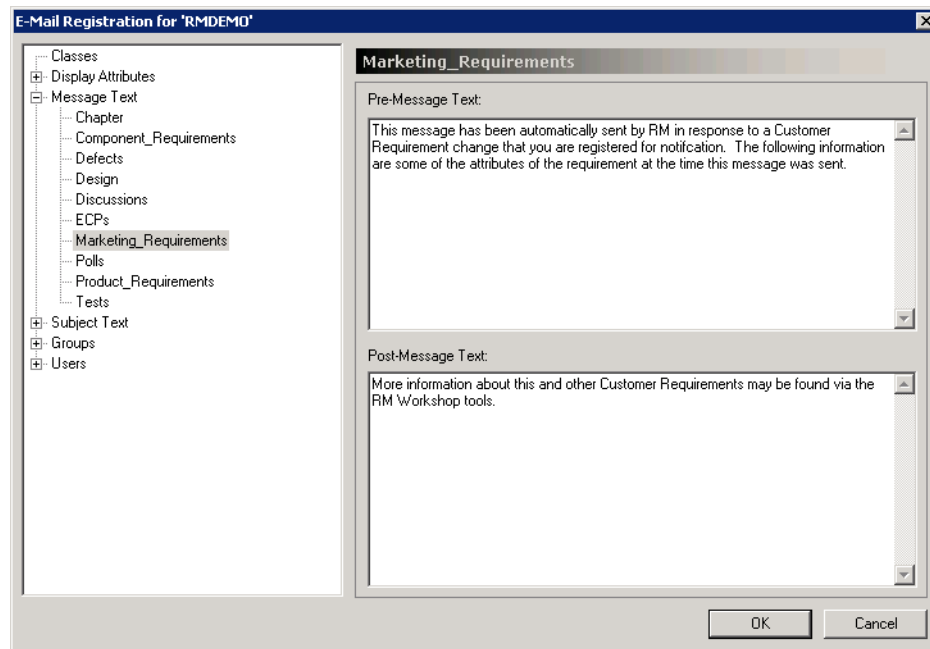
2　Enter the pre-message and post-message text into the appropriate field in the right pane.

NOTE Attribute values cannot be included in this text.

To define default pre-message and post-message text:

1　Select the **Message Text** branch.

2　Enter text as described earlier in this section.

Defining the Default Subject Text

You can define a the text that goes into the subject line for the e-mail for each class. The subject text can contain placeholders for attribute values that will be expanded before the e-mail is sent. Default subject text can be defined for all classes that do not have a specific subject line.

To define the default subject text:

1　Do one of the following:

> **a** If you want to define the subject text for all classes, select the **Subject Text** branch.
>
> **b** If you want to define the subject text for one class, expand the **Subject Text** branch and select the appropriate class.
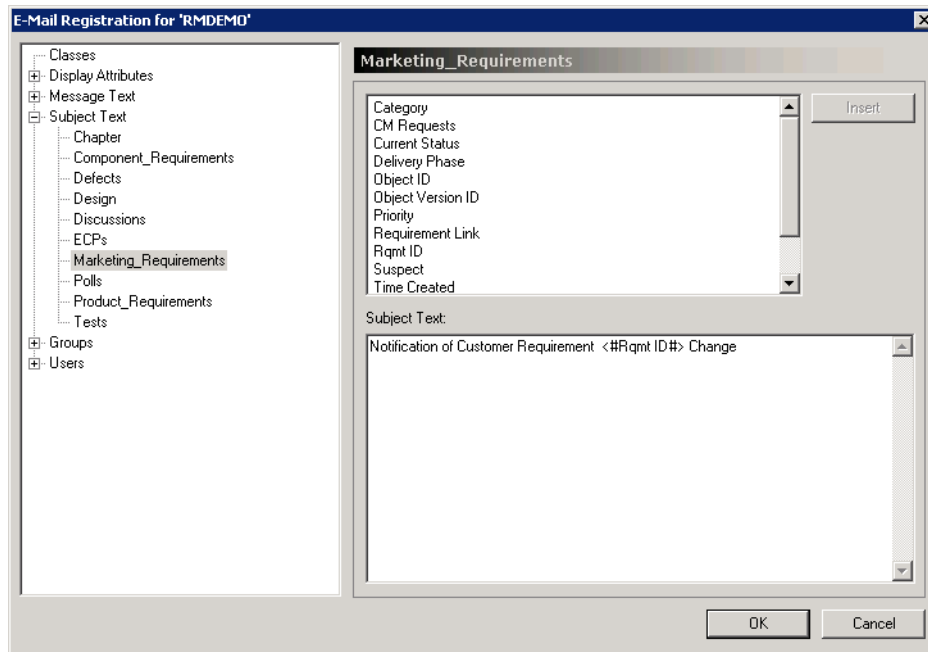
2 Type the subject text.

3 To include an attribute value in the subject line, either select the desired attribute from the list shown above the subject text and click **Insert** or type the attribute's display name into the string surrounded by the strings <# and #>.

Enabling Group Rules

You can define which groups have e-mail notifications enabled. The RM Mail service only processes rules for groups that have e-mail notification.

Disabling e-mail notification for a group does not delete the rules that have been defined by the group. It simply suppresses the processing of rules for the group.

To enable or disable e-mail notification for a group:

1 Select the **Groups** branch.
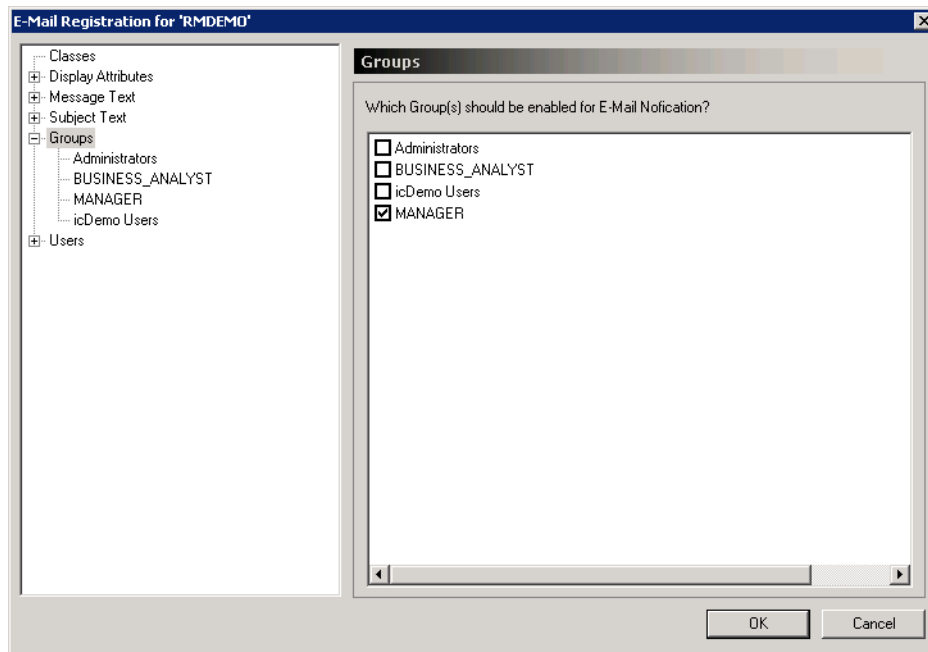
Group rules that are enabled have a selected check mark next to them, and group rules that are disabled have a cleared check box next to them.

2 Select the check box to the left of the group to enable e-mail notification, or clear the check box to disable e-mail notification.

3 If you enabled group rules, ensure that group rules exist and they are enabled (see chapter "Editing Group Rules" on page 247).

Editing Group Rules

The instance administrator has access to the rules created for all groups. As a result, the administrator can add, modify, or delete rules for any group that have been assigned to the instance.

To edit group rules:

1   Expand the **Groups** branch and select a group.
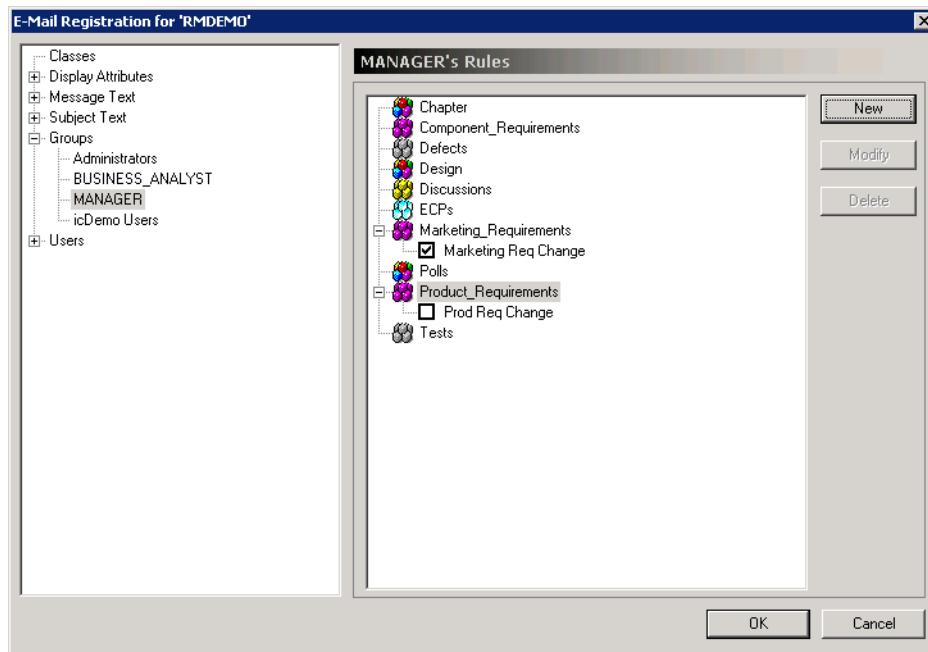
The right pane will show a list of all classes that can be expanded to show the rules that have been created for the class. Rules that are enabled have a selected check box next to them, while rules that are disabled have a cleared check box next to them.

2   Click the check box to the left of the desired rule to enable or disable rules.

Enabling User Rules

You can define which users have e-mail notifications enabled. The RM Mail service only processes rules for users that have e-mail notification.

You typically disable e-mail notification temporarily for users while they are on vacation. Disabling e-mail notification for a user does not delete the rules that have been defined by the user. It simply suppresses the processing of rules for the user.

To enable or disable e-mail notification for a user:

1   Select the **Users** branch.
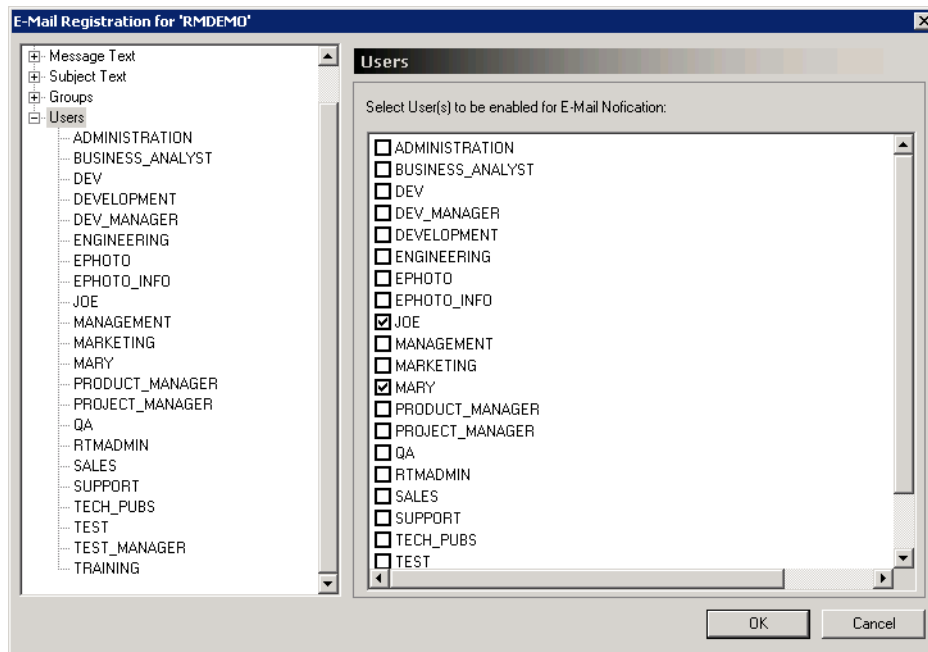
User rules that are enabled have a selected check mark next to them, and user rules that are disabled have a cleared check box next to them.

2   Select the check box to the left of the user to enable e-mail notification, or clear the check box to disable e-mail notification.

3   If you enabled user rules, ensure that user rules exist and they are enabled (see chapter "Editing User Rules" on page 249).

Editing User Rules

The instance administrator has access to the rules created by all users. As a result, the administrator can add, modify, or delete rules for any users that have been assigned to the instance.

To edit user rules:

1   Expand the **Users** branch and select a user.
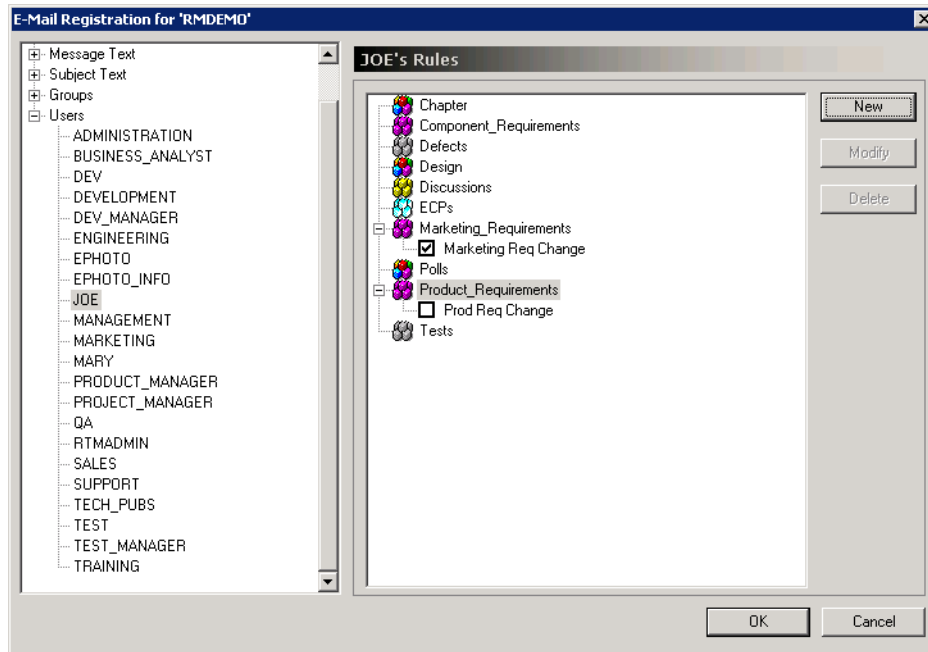
The right pane will show a list of all classes that can be expanded to show the rules that have been created for the class. Rules that are enabled have a selected check box next to them, while rules that are disabled have a cleared check box next to them.

2   Click the check box to the left of the desired rule to enable or disable rules.

Creating a Rule

The following sections describe the E-Mail Rules wizard, which guides you through the creation of a new rule.

To create a rule:

1   In **RM Manage**, in the **E-Mail Registration** dialog box, select the class for which the rule should be created.

2   Click **New**. This opens the **E-Mail Rules Wizard** dialog.

3   Enter a name for the rule in the **What should the rule be called?** field. This name will later be shown in the tree control.

4   Change the **Subject Text** as desired. The initial subject text is the text you defined in chapter .

5   If you want the created rule to be disabled, clear the **Enable this rule?** box.

Defining the Trigger Condition

The second step of creating a new rule is to define the triggering condition for when the e-mail should be sent:

The triggering conditions falls into the following two broad categories:

■ **When an object created by me is modified**

Choose this option if you want to be notified whenever an object that you create has been changed. This will trigger an e-mail to be sent to you regardless of the change. If this option is selected, the remainder of the items on the page are hidden because they are no longer applicable.

■ **When attribute has value...**

Choose this option to specify that an e-mail should only be sent if the specified set of constraints are met.

To add constraints, do the following:

a Select the attribute from the **Attribute** drop-down list.

b Select one constraint from the **Constraint** drop-down list:
Is: The value of the attribute must match the value from the **Value** drop-down list.
Is Not: The value of the attribute must not match the value from the **Value** drop-down list.
Null: The value of the attribute must be null (empty).
Not Null: The value of the attribute must not be null (empty).

c Select the value for the specified constraint from the **Value** drop-down list.
Multiple constraints can be added and these constraints are totaled to determine if

an e-mail should be sent. Constraints can only be added to list attributes, user attributes and **the Category attribute.**

> **NOTES**
>
> - The **Value** drop-down list is only available if the **Is** or **Is Not** is selected in the **Constraint** drop-down list.
>
> - The **Null** and **Not Null** constraints are not available for the Category attribute.

    d For Date attributes, you can specify at which day the notification e-mail shall be sent. To specify the date, on which the e-mail shall be sent, the system uses the values from **Operator** and **Days** to calculate the date in the selected field. If this matches, the notification e-mail will be sent.

    Example:

    Your requirement has a Date attribute which is set to December 1st.
Your constraint defines: Is <Current Date> - 1 Days.
This means that you will receive your e-mail on the next day, December 2nd.

    e When selecting the Category Attribute, select **Include subcategories** to match also **all** subcategories of the selected category.

- **When Comment is added and attribute has value...**

    Choose this option to specify that an e-mail should only be sent if a comment has been added to a requirement and the specified of constraints are met.

    To add constraints, do the following:

    a Select the attribute from the **Attribute** drop-down list.

    b Select one constraint from the **Constraint** drop-down list:
    Is: The value of the attribute must match the value from the **Value** drop-down list.
    Is Not: The value of the attribute must not match the value from the **Value** drop-down list.
    Null: The value of the attribute must be null (empty).
    Not Null: The value of the attribute must not be null (empty).

    c Select the value for the specified constraint from the **Value** drop-down list.
    Multiple constraints can be added and these constraints are totaled to determine if an e-mail should be sent. Constraints can only be added to list attributes, user attributes and the Category attribute.

> **NOTES**
>
> - The **Value** drop-down list is only available if the **Is** or **Is Not** is selected in the **Constraint** drop-down list.
>
> - The **Null** and **Not Null** constraints are not available for the Category attribute.

    d For Date attributes, you can specify at which day the notification e-mail shall be sent. To specify the date, on which the e-mail shall be sent, the system uses the values from **Operator** and **Days** to calculate the date in the selected field. If this matches, the notification e-mail will be sent.

    Example:

Your requirement has a Date attribute which is set to December 1st.
Your constraint defines: Is <Current Date> - 1 Days.
This means that you will receive your e-mail on the next day, December 2nd.

e When selecting the Category Attribute, select **Include subcategories** to match also **all** subcategories of the selected category.

Defining the Attributes to be Monitored

If you selected **When attribute has value ...** in the previous step, you must determine which attribute should be monitored for a change in value. The mail service only processes a rule if the values change for attributes selected in this step.

This page of the **E-Mail Rules Wizard** is not displayed if you selected **When object created by me is modified** in the previous step, because an e-mail is sent regardless of which attributes change.

Selecting the Attribute to Include in the E-Mail

Finally, you need to determine which attributes to include in the e-mail. The list on the left contains a list of attributes that will not be included with the e-mail, while the list on the right displays a list of attributes that will be included.
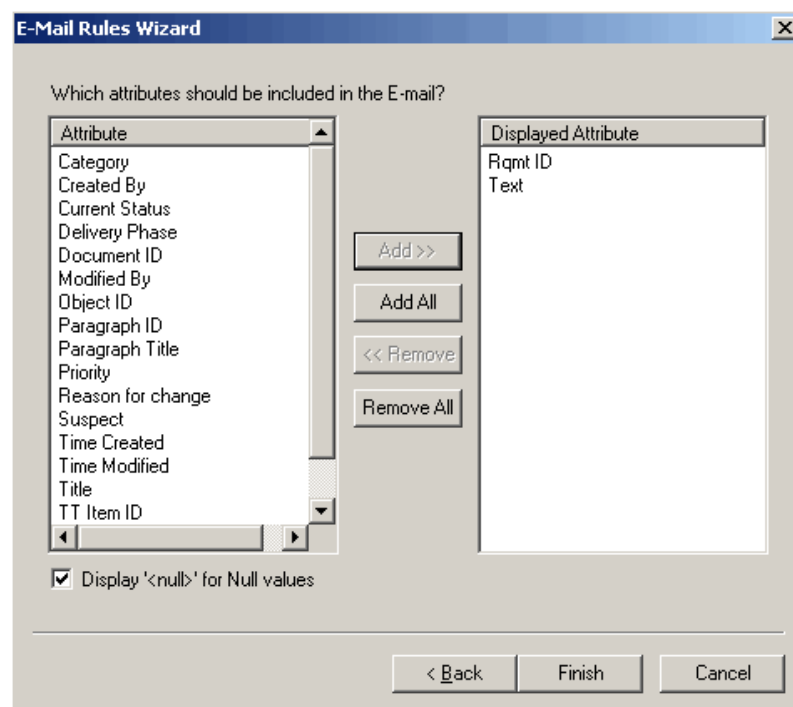
To add an attribute to the list of attributes included with the e-mail, either double-click the attribute in the left hand list or select the attribute and click **Add**. To remove an attribute from the list of attributes included with the e-mail, either double-click the attribute in the right list or select the attribute and click **Remove**.

Dragging and dropping the attributes in the **Displayed Attribute** list changes the order in which the attributes are included in the e-mail. Note that the attributes are included in the e-mail in the order they appear in the **Displayed Attribute** list.

The values for the administrator-defined attributes will be included in the e-mail prior to the attributes that you select to display when creating a rule.

If the **Display <null> for Null values** check box is selected, the string "<Null>" is included next to the attribute display name in the e-mail if the attribute does not have a value assigned to it. If it is not selected, nothing will be displayed after the attribute display name.

Modifying a Rule for a Group

To modify a rule for a group:

1 Expand the **Groups** branch.

2 Select the group.

3 In the right-hand pane, expand the class for which the rule is defined.

4 Select the rule.

5 Click **Modify** to run the **E-Mail Rules Wizard**.

Modifying a Rule for a User

To modify a rule for a user:

1 Expand the **Users** branch.

2 Select the user.

3 In the right-hand pane, expand the class for which the rule is defined.

4 Select the rule.

5 Click **Modify** to run the **E-Mail Rules Wizard**.

Deleting a Rule for a Group

To delete a rule for a group:

1 Expand the **Groups** branch.

2 Select the group.

3 In the right hand pane, expand the class for which the rule is defined.

4 Select the rule.

5 Click **Delete**.

Deleting a Rule for a User

To delete a rule for a user:

1 Expand the **Users** branch.

2 Select the user.

3 In the right hand pane, expand the class for which the rule is defined.

4 Select the rule.

5 Click **Delete**.

RM Mail Service

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:

- **NT 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. In order to install the RM Mail server components, you must perform a custom installation and install the *RM Mail* component.

- **Configuration Panel Applet**—The system on which RM Mail is installed has a Windows applet that is used to configure the various aspects of the mail service.

- **Rule Configuration**—Instance administrators and users must configure the e-mail rules processed by RM Mail.

> **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 | Micro Focus | 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 256).

- **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 257).

- **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 258).

- **Log:** Used to configure the amount of log information that is appended to the system application log (see "Log Tab" on page 260).

- **Notifications:** Used to inform administrators about administrative activities, e.g. creation of users or groups (see "Notifications Tab" on page 261).

- **General:** Used to specify the RM Browser URL for RM Mail service (see "Log Tab" on page 260).

2 Specify RM mail settings.

3 Click **Apply**.

4 Stop and then restart the **Micro Focus Dimensions RM E-Mail Service** service.

This can be done from the following locations:

- RM Mail **Control** tab (see "Control Tab" on page 258)

- Windows **Services** (from the Windows **Control Panel**, double-click **Administrative Tools** and then double-click **Services**).

Database Tab

Initially, the list of instances will be blank until a database location is selected from the **Database Location** drop-down list. When a database location is selected, a list of all Dimensions RM instances resident at that location is displayed.
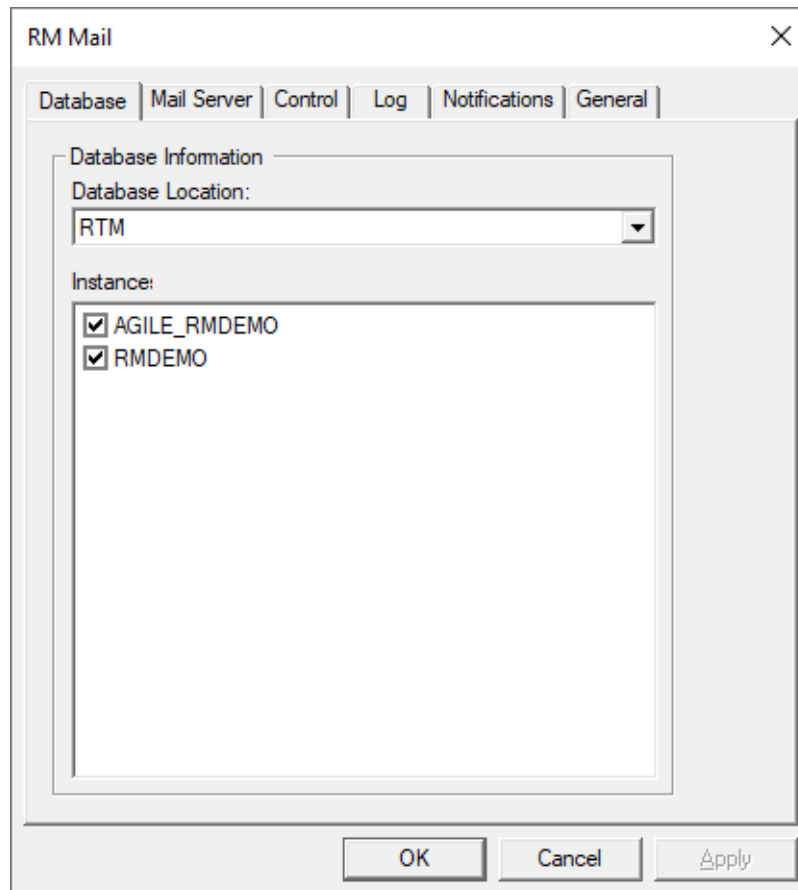
In the check box next to each instance, select the instances this service should monitor. The mail service can monitor multiple instances at many locations.

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. You typically disable notifications when performing tasks such as batch updates.

Mail Server Tab

For the RM Mail service to send e-mail, it must have access to an SMTP mail server that has already been set up on the network.

Fill the fields of the dialog as required or desired:

Field	Description
Server Name (SMTP):	The name or IP address of the SMTP server
Server Port:	The port used for communication with the SMTP server
Use TLS:	If enabled, TLS security will be used. The used version depends on the TLS version supported by the SMTP server.
Use Authentication:	Enable this option, if the SMTP server requires a user name and password.
Authentication Mode:	The authentication mode depends on the SMTP server. ■ **Login:** Transmits user name and password individually. ■ **Plain:** Transmits user name and password together.
Login:	A user name that is accepted by the SMTP server.
Password:	The password for the SMTP user name.

Field	Description
Name:	Specify the name you want users to see as the sender's name, e.g. *Dimensions RM Administrator*. You may leave this field empty if you do not wish to reply.
E-Mail Address:	Specify the e-mail address you want users to be able to reply to. You may leave this field empty if you do not wish to reply.

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.
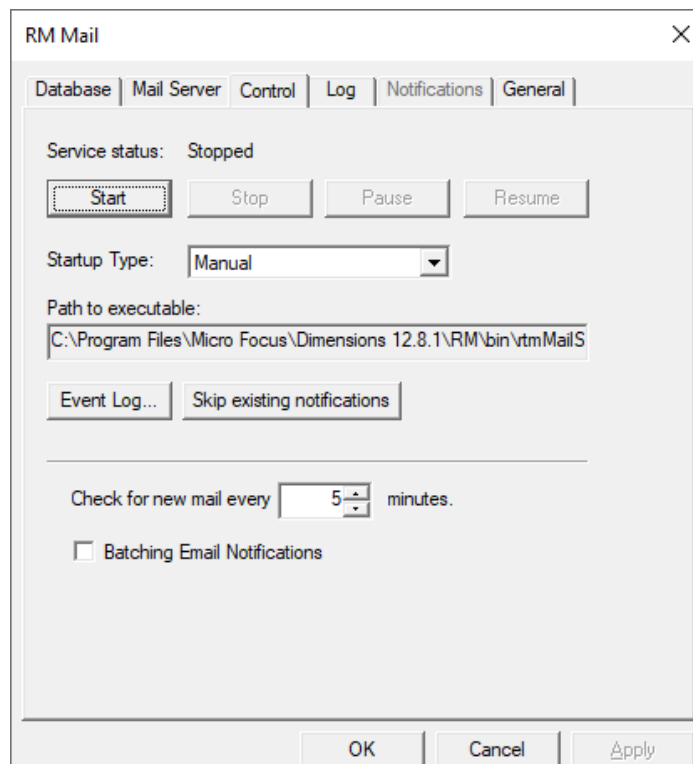
The current status of the service is displayed at the top of the dialog box.

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.

The path to the *rtmMailService.exe* executable is provided for reference.

Click **Event Log** to view a list of events that have been logged by the RM Mail service.

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.
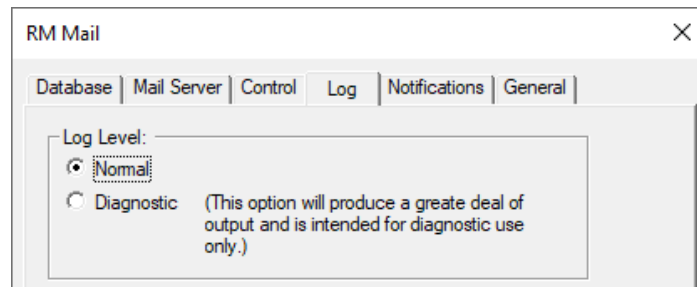
The default log level is **Normal**, which logs a minimum of information to the system application log and is the recommended option for normal use.

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

The notifications tab allows you to configure to send e-mails to one or several e-mail addresses when certain system activities (e.g. creation of user accounts) occur.

> **NOTE** To allow configuration on the Notifications tab, the RM Mail service must be configured and running.

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.
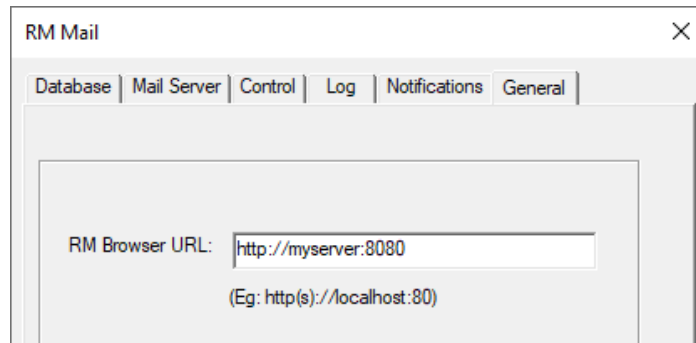
Configuring Login Sources

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 Micro Focus SSO server (the Micro Focus 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 Micro Focus 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 you 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 company or corporation domain.

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

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 267.

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.
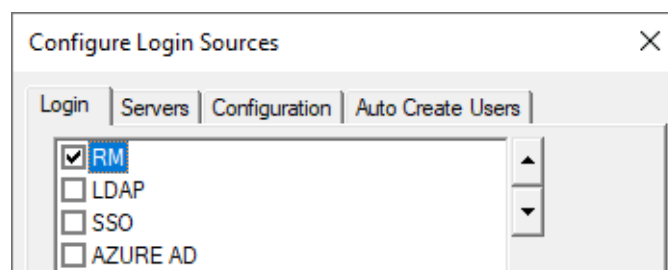
4 Select the login sources that you want Dimensions RM to use.

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 267.

■ **SSO:** Note that before you can use SSO with your RM clients, you must configure the RM server to connect to the Micro Focus 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 264.

■ **AZURE AD:** Proceed to "Specifying the Azure AD Configuration" on page 274.

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 Micro Focus 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.

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 218) 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 **Micro Focus 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 mor 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" on page 263.

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 **Micro Focus 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 ![icon] , 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 ![icon] , 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.

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 264.

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 268).

2 Specify the related LDAP servers in RM Manage (see chapter "Specifying an LDAP Server" on page 267).

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_NAMIMG_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_NAMIMG_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_NAMIMG_ATTRIBUTE: **User Naming Attribute**
>
> - BIND_ANONYMOUSLY: **Bind Anonymously**. To enable, set 1; to disable set 0.
>
> - USER_DN: **User DN**
>
> - USER_PASSOWRD: **Password**
>
> For reference of the above settings, refer to chapter "Specifying the LDAP Configuration" on page 268.

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. myldapserver.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 ![icon] , 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. myldapserver.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:
> - Open a command prompt.
> - Enter `tracert` followed by the fully qualified server name (e.g. `tracert myldapserver.mydomain.com`).
> - 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.

6 Click **Apply**.

7 Select the **LDAP Configuration** tab.

8   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 268).

9   Click **OK** to update the information within your RM instances database.

10   Select the **LDAP Servers** tab.

11   Click **Test**. You should receive the message **LDAP Test Connection successful.**

12   LDAP is now configured to use SSL.

Specifying the Azure AD Configuration

Before you begin, ensure that you have registered with Azure AD and that you have the login for the administrative account.

Configuring Azure AD

If you are using Azure AD as a login source, you must specify an Azure AD configuration.

> **IMPORTANT!** Before you start, do the following:
>
> ■   Ensure that you have the admin login data for Azure.
>
> ■   Ensure that you registered your Dimensions RM server as Azure app (see chapter "Registering Dimensions RM as Azure Application" on page 550).
>
> ■   Ensure that you retrieved all required values as described in chapter "Retrieving Configuration Data from Azure AD" on page 551.

To configure an Azure AD:

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   Select **AZURE AD** in the list and click **Settings**. This opens the Azure AD Settings dialog.

3   **Enter the following settings:**

    a   **Tenant:** Enter the value you retrieved in point 3c of chapter "Retrieving Configuration Data from Azure AD" on page 551.

    b   **Client ID URI:** Enter the value you retrieved in point 4e of chapter "Retrieving Configuration Data from Azure AD" on page 551.

    c   **Client ID:** Enter the value you retrieved in point 4f of chapter "Retrieving Configuration Data from Azure AD" on page 551.

    d   **Issuer URL:** Enter the value you retrieved in point 5e of chapter "Retrieving Configuration Data from Azure AD" on page 551.

   e **Trust Certificate:** Enter the full path (including the file name) to the certificate you retrieved in point 6g of chapter "Retrieving Configuration Data from Azure AD" on page 551.

4 **If you use authentication method OAuth, do the following:**

   a Select **OAuth**.

   b Click **Settings**. This opens the **OAuth Settings** dialog.

   c Enter the value you retrieved in point 5d of chapter "Retrieving Configuration Data from Azure AD" on page 551.

   d Click **OK** to close the **OAuth Settings** dialog.

5 Click **OK** to close the **Azure AD Settings** dialog.

6 Ensure that the **AZURE AD** entry in the Login Sources list is selected.

7 Click **OK** to close the **Configure Login Sources** dialog.

> **NOTE** To configure the login page to use Azure as default login method, see chapter "Configuring Azure Login for the Login Page" on page 391.

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" on page 263).

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 204) 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. **NOTE** When you reset the password for an existing user, this setting is not validated.

Setting	Description
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.
Minimum number of special characters	The minimum number of special characters that a password must contain. The following special characters are allowed: ! " # $ % & ' ( ) * + , - _ / : ; < = > ? [\ ] ^ { | } ~ ` The maximum number for this setting is 99.
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.

Setting	Description
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.
Minimum number of special characters	The minimum number of special characters that a password must contain. The following special characters are allowed: ! " # $ % & ' ( ) * + , - _ / : ; < = > ? [\ ] ^ { | } ~ ` The maximum number for this setting is 99.
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.

Setting	Description
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.	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. Alternatively, to assign an alternative date for password rules to be enforced, either: ■ select and overtype, as appropriate, the day, month, and year; or ■ click the down-arrow and use the calendar dialog box that appears.

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.	`icmanage -user user -password password -location database -project instance -buffer buffer -dumpfile dumpfile`
	Back up (Oracle database)	`icmanage -location <database instance name> -project <instance name> -password <instance password> [-buffer <buffer size>] -dumpfile <name and path of backup file to be created>`
	Back up (SQL Server database)	`icmanage -location <database instance name> -rmdbapassword <instance password> -dumpfile <name and path of backup file to be created>`
	Amazon cloud RDS mode	`icmanage -aws` The other command line options (as described above) can be used in combination with the `aws` option.
Synch Engine	Run the Synch Engine	`syncengine [-f file] [-c] [-e level] [-E file] [-L priority] [-k {install|config|uninstall|start|stop}] [-n serviceName] [-v] [-h] [-p password] [-P eventName]`
ALF Emitter	Run ALF emitter service, see "Application Lifecycle Framework (ALF)" on page 139	`ALFEventEmitter [-f file] [-c] [-e level] [-E file] [-L priority] [-k {install|config|uninstall|start|stop}] [-n name] [-v] [-h]`
Class Definition	Launch class definition.	`clasdef -user user -password password -location database -project instance`

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.

Icons and Toolbars

Icons

The following table describes the icons.

Icon	Description
	Database
	Instance
	Offline Instance
	User
	Group
	Granted Access Rights
	Denied Access Rights
	Inherited Access Rights

Toolbars

This section describes the toolbars of RM Manage.

Main Toolbar

The following table describes the buttons of the **Main** toolbar.

Button	Action
	View instance information
	View group information
	View user information
	Show Help topics

Database Toolbar

The following table describes the buttons of the **Database** toolbar.

Button	Action
	New instance
	Change user
	Change user password

Button	Action
	Configure login sources
	Convert database
	Administer tablespaces
	Properties
	Create ICDBA Account
	Change Administrator Password
	Change Encryption Keys

Instance Toolbar

The following table describes the buttons of the **Instance** toolbar.

Button	Action
	Change instance password
	Delete instance account
	Define instance schema
	Backup or restore instance account
	Backup or restore instance schema
	Place instance account online
	Place instance account offline
	Install instance tables
	Drop instance tables
	Recreate database procedures
	Recreate database indexes
	Recreate resources
	Administer email
	Administer locks
	Associate to Dimensions CM
	(Show) Properties
	Baseline link(s)

Group Folder Toolbar

The following table describes the button of the **Group Folder** toolbar.

Button	Action
	New group

Group Toolbar
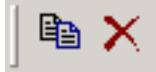
The following table describes the buttons of the **Group** toolbar.

Button	Action
	Copy group
	Delete group

User Folder Toolbar

The following table describes the button of the **User Folder** toolbar.

Button	Action
	New user

User Toolbar

The following table describes the buttons of the **User** toolbar.

Button	Action
	Copy user
	Delete user

Chapter 9
Class Definition

Overview

> **CAUTION!** All users must be off the system before making any changes in Class Definition to preclude schema changes during user operations. There should *never* be an exception to this rule on a production system.
>
> It is best practice, before saving from class definition, to always:
>
> **1** Stop the Micro Focus Common Tomcat service.
>
> **2** Stop the Micro Focus Dimensions RM Pool Manager service.
>
> **3** Review and drop all locks.
>
> **4** Backup instances.
>
> **5** Post/save Class Definition changes.
>
> **6** Start the Micro Focus Common Tomcat service.
>
> **7** Start the Micro Focus Dimensions RM Pool Manager service.

The class definition process, also known as the schema creation process, is the first step in Dimensions RM instance management. This process sets up instance flows and logical groupings of information and is the responsibility of the instance administrator.

Defining classes for an instance enables you to perform the following functions:

- Organize information according to meaningful categories (classes).

- Qualify the information within each class according to attributes you define for the class. This enables you 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.

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

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).

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.
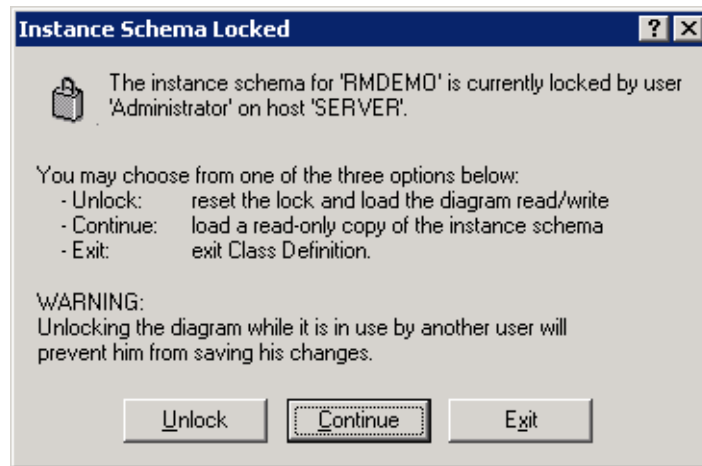
Figure 9-1. Instance Schema Locked

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.
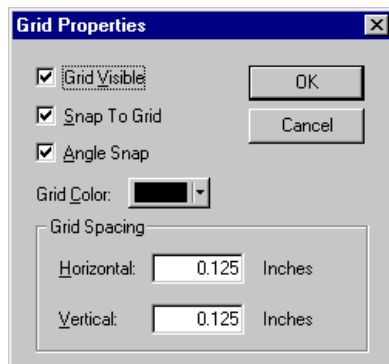
Figure 9-2. Grid Properties

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.
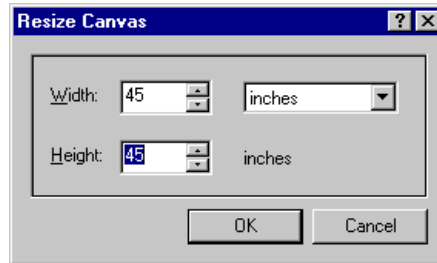
Figure 9-3. Resize Canvas

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.
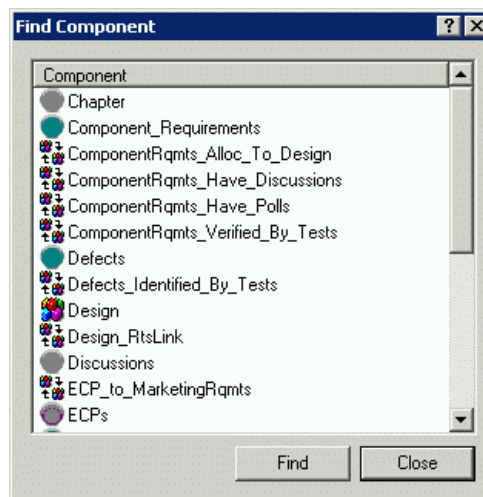
Figure 9-4. Find Component

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.

田	Nudge Up
田	Nudge Down
田	Nudge Left
田	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. You can define any number of attributes for each class and relationship. In addition to these user-defined attributes, there are implicit predefined 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**
A1	Alphanumeric	A single line of text up to 1000 characters.	299
	Date	A date, the format of which (including length, default, minimum, and maximum values) can be defined by the administrator.	300
	File Attachment	Can hold one or several files to be accessed from RM Browser.	300
	Group	Like a list attribute, but composed of a series of sub attributes. The choices available to the user *depend* upon the selections they made in the higher level, or parent, attributes within the group attribute.	301
	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.	305
Q	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.	310
1.2	Numeric	Accepts only numeric values.	312
T	Text	A block of text up to 64Kb in size.	313
	URL	Allows to specify one or several URLs.	313
	User	A list of user names, which can be configured by group or individual user names.	314

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. **NOTE:** 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 "RRRR Date Format Elements" on page 352.

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
Allow multiple selections	Whether the attribute can hold one or multiple files. ■ Enabled: The attribute can hold multiple files. ■ Disabled: The attribute can hold a single file.

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 304.

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).
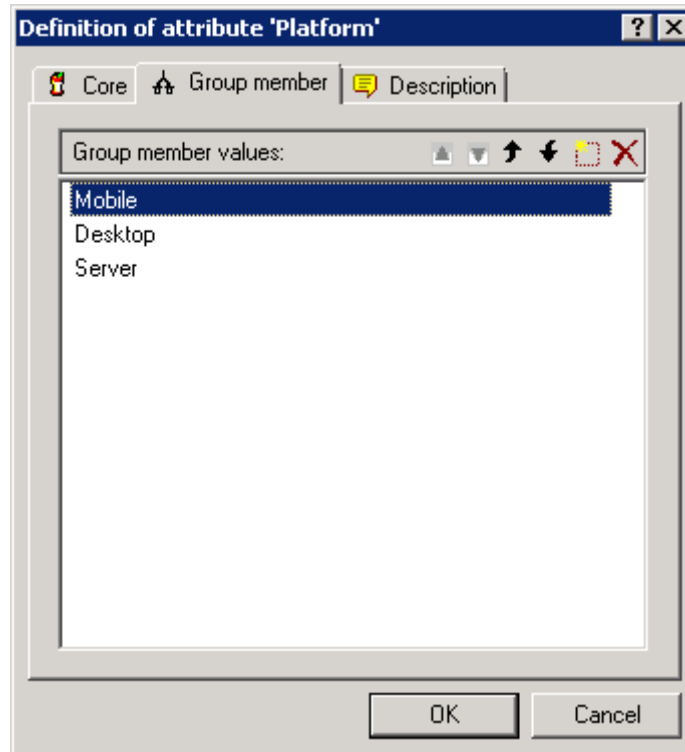
2 To add members (sub attributes) to the group attribute, click the **New** button (or press the **Insert** key) and enter a name. The name must be unique within the group attribute.
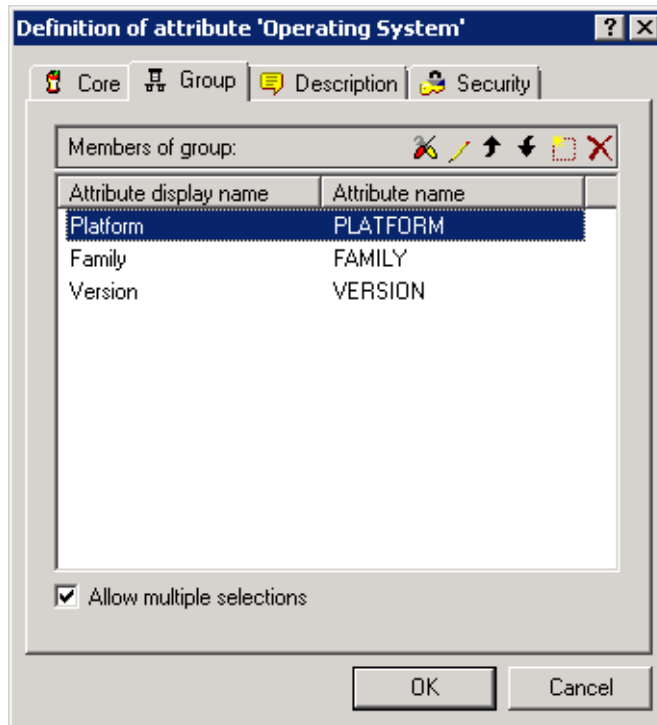
To delete a member attribute from the group, highlight the attribute and click the **Delete** button, or press the **Delete** key.

3 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.

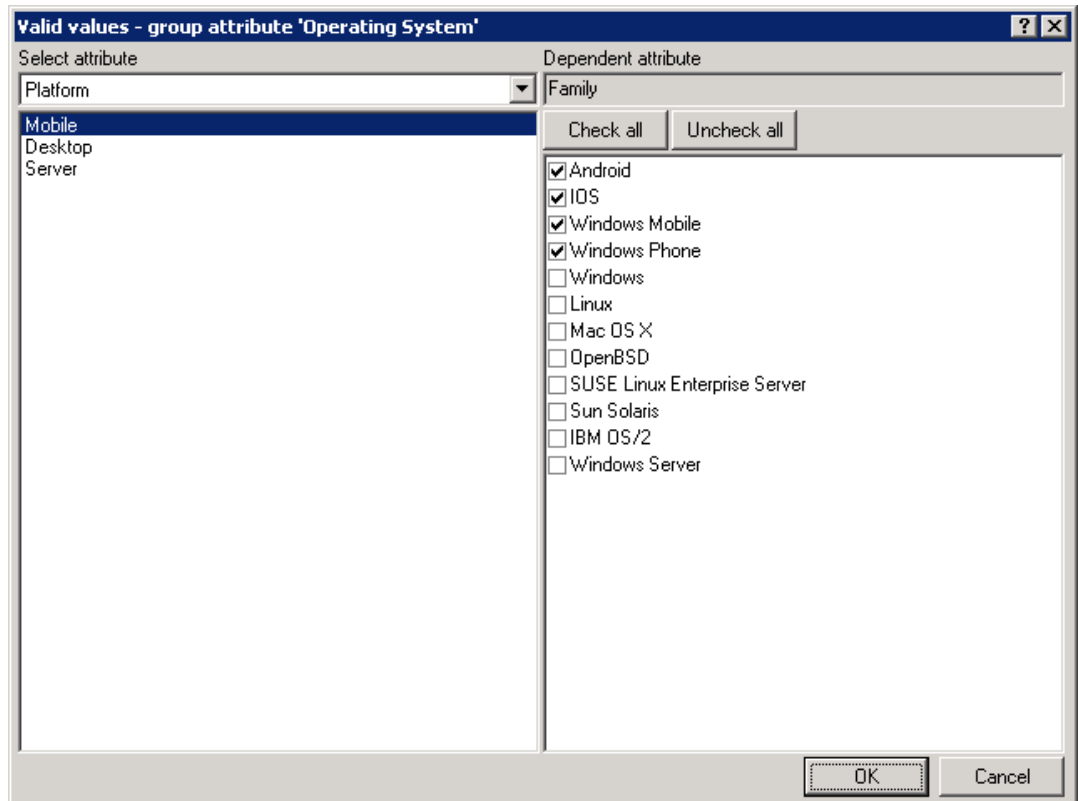**c** Once you have defined and ordered the values for a group member, click the **OK** button to return to the Definition of attribute dialog for the group attribute (which has a **Group** tab rather than the **Group member** tab).

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.
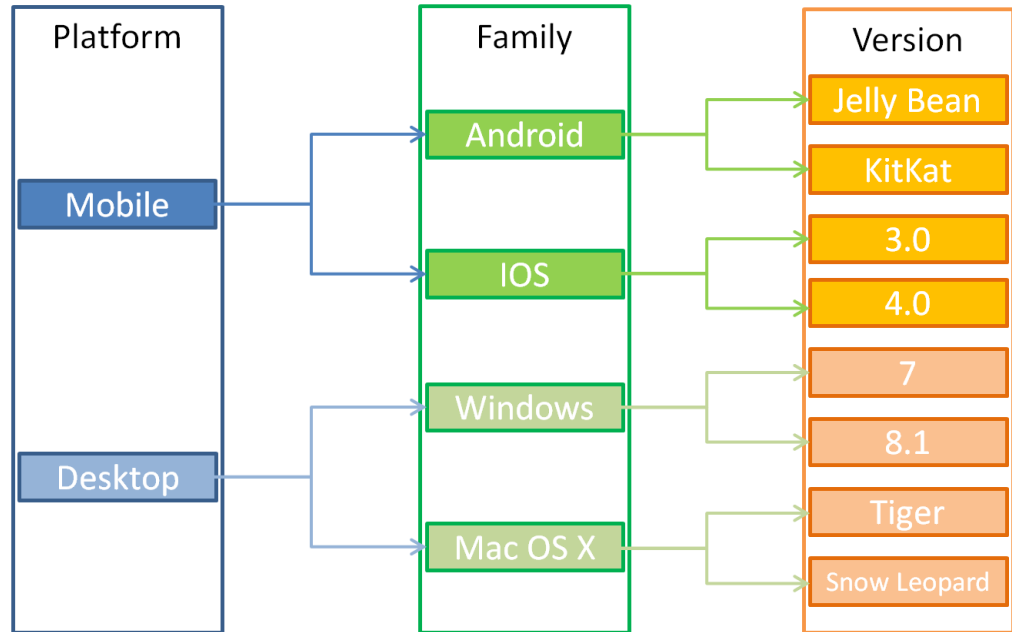
The group attribute contains the group members **Platform**, **Family**, and **Version**. By restriction, you can define which values the user will see when selecting a value. The selection of the **Platform** group member defines the values of the **Family** group member. The selection of the **Family** 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.
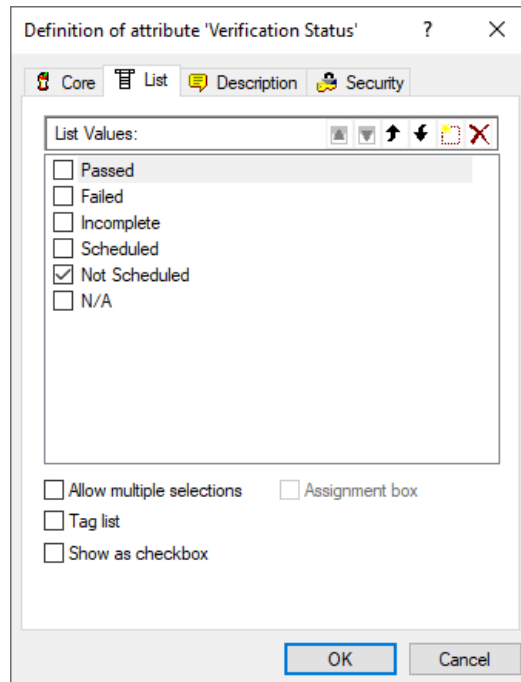
Figure 9-7. List Attribute Definition

A list attribute can also be configured to display as a checkbox or radio buttons.
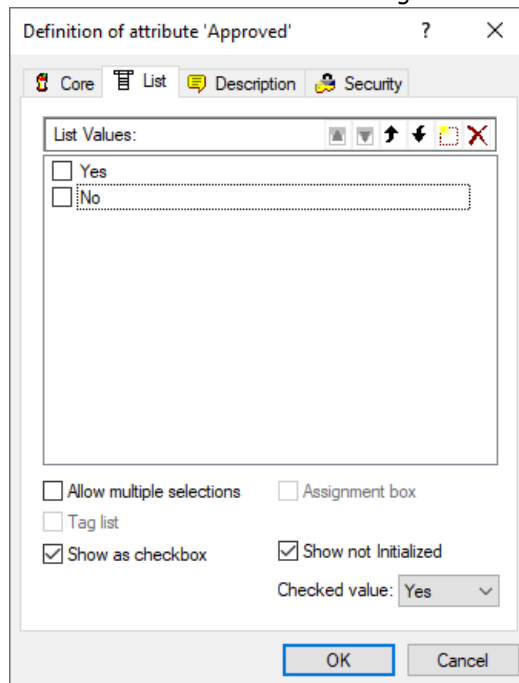
Figure 9-8. List Attribute Definition as Checkbox

The list attribute properties are described in the following table.

Property	Description
List Values	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.
Allow multiple selections	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.
Assignment box	Only available when **Allow multiple selections** is selected and **Tag list** is not selected. Enabling this option replaces a single list with two lists which allow adding/removing entries by using ➡ and ⬅ .
Tag list	Attribute values are displayed as "tags". Enabling this option also means that each user having write access can add values to this attribute. **CAUTION!** 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 **strongly** suggested to make changes to the class definition outside business hours.
Show as checkbox	The list attribute is displayed as checkbox or radio buttons. For further details, see chapter "Configuring a List Attribute as Check Box / Radio Button" on page 309.
Show not Initialized	Show the option **Not Initialized** for a radio button or the text **Not Initialized** for a checkbox. For further details, see chapter "Configuring a List Attribute as Check Box / Radio Button" on page 309.
Checked value	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 309.

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 trial 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 as Check Box / Radio Button

Check boxes or radio buttons are configuration options for the list attribute. See chapter 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.
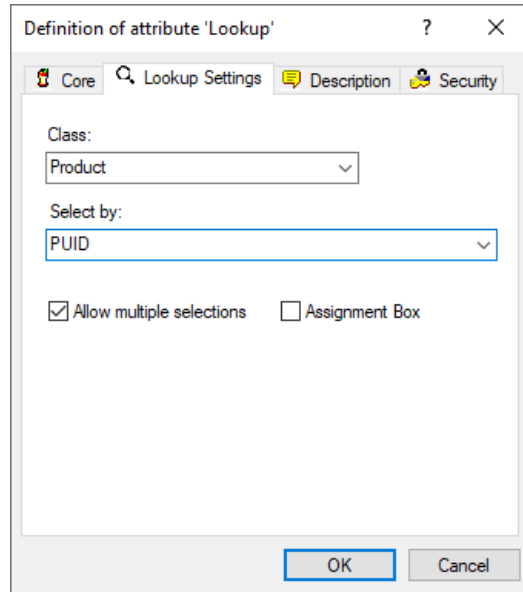
Figure 9-9. Lookup Attribute Definition

The properties are described in the following table:

Property	Description
Class	The class that relates to the current class.
Select by	The attribute that provides the values for the list.
Allow multiple selections	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.
Assignment Box	Only available when **Allow multiple selections** 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.
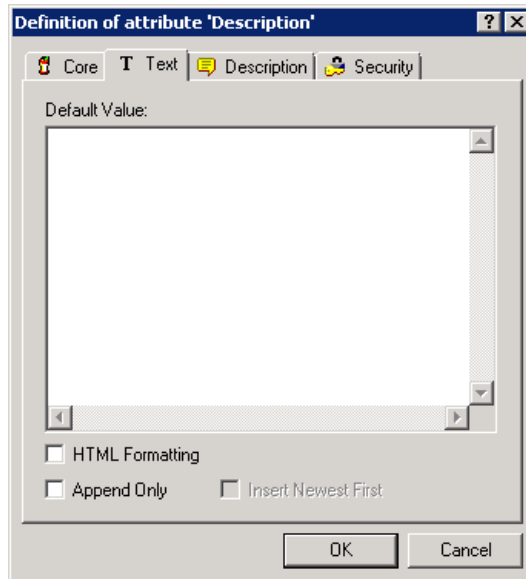
Figure 9-11. Text Attribute Definition

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. **NOTE:** 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	■ **Single:** The URL attribute can only hold one URL. ■ **Multiple:** The URL attribute can hold several URLs.
Limit count to	This option is only available if **Mode** is set to **Multiple**. Select this option and specify any value higher than 0 to define the maximum number of URLs the attribute can hold.
Validation pattern	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: ■ `^(http[s]?|ftp):\/\/(.*)` The URL must use either the HTTP, HTTPS or FTP protocol. ■ `^https:\/\/www\.microfocus\.com\/(.*)` The URL must use the HTTPS protocol and the server must be www.microfocus.com.
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.
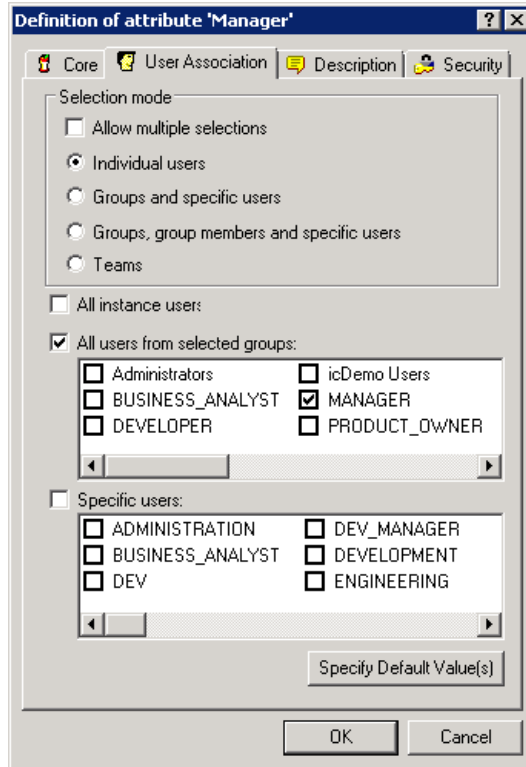
Figure 9-12. User Attribute Definition

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 **All users from selected groups list** and users specified in the **Specific users** list can be selected.
Groups, group members and specific users	Groups selected in the **All users from selected groups list**, users who are members of the selected groups and users specified in the **Specific users** 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*.
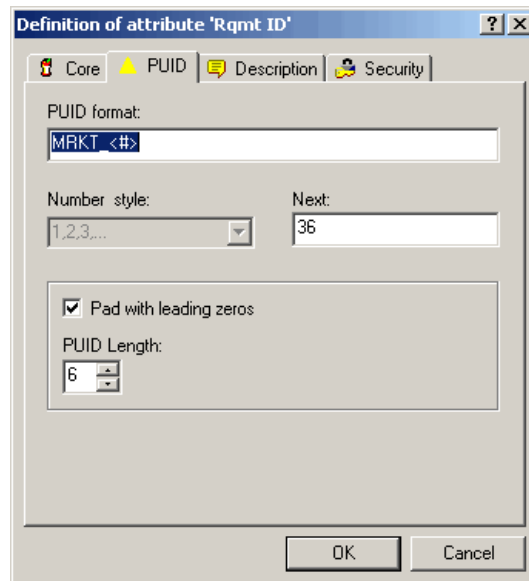
Figure 9-13. Rqmt ID Attribute Definition

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. **NOTE:** 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.
Pad with leading zeros	Whether zeros precede the PUID to make the PUID number the number specified in the **PUID Length** list.
PUID Length	The number of numbers that can replace the <#> variable.

NOTE The PUID tab is displayed only if the class is empty (no objects/requirements exist in 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 298.

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.
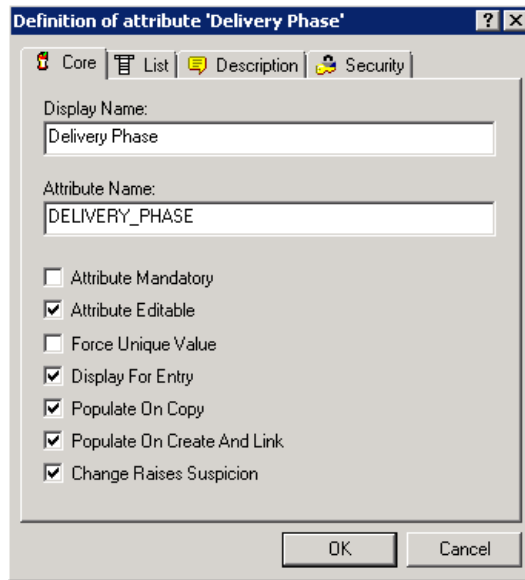
Figure 9-14. Attribute Definition

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 "Naming Conventions for Attribute Display Names" on page 30.
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 "Naming Conventions for Attribute Names" on page 31.
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 used for security.

Property	Description
Populate on Copy	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 *not* to copy the Title and Description attributes. When using **Populate on Copy** 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.
Populate on Create and Link	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 "Transfer Rules" on page 334).
Change Raises Suspicion	This setting is available for any custom attribute and the following system attributes: ■ **Category:** The **Category** attribute changes when a requirement is moved to a different category. ■ **Class ID:** The **Class ID** attribute changes, when a requirement is changed to a different class (e.g. *Marketing_Requirements* to *Product_Requirements*). ■ **Owner:** The **Owner** attribute of a requirement an be changed by a workflow transition ■ **Workflow State:** The **Workflow State** attribute changes when a requirement is transitioned to a different state. If this setting is enabled, any replace action on this attribute will mark linked objects as **Suspect** if this is enabled in the relationship definition (see chapter "Transfer Rules" on page 334).

Attribute Type Tab

The second tab is specific to the attribute type selected in Step 2 on page 317. The attribute type tabs are described under "Attribute Types" on page 298.

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 342.

> **NOTE** You can edit an attribute definition at any time after having defined it. This could mean that values of the attribute are no longer valid for certain instances of the class. For example, if a Force Unique Value property is added to a numeric attribute, existing values of this attribute that are not unique must be identified and altered by making it unique through replacement or batch update.

Deleting an Attribute

To delete an attribute from a class or relationship definition:

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 30.

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.
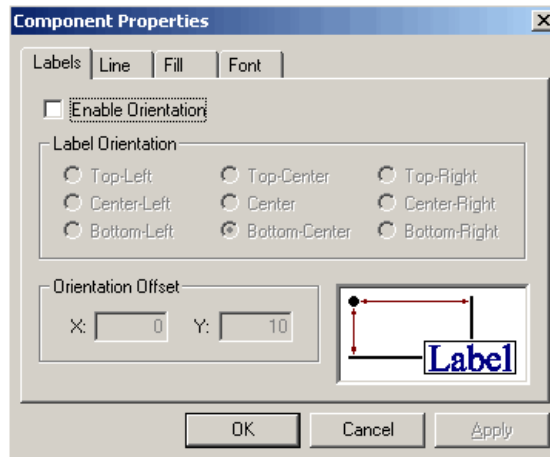
Figure 9-15. Component Properties

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 324).

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 30.
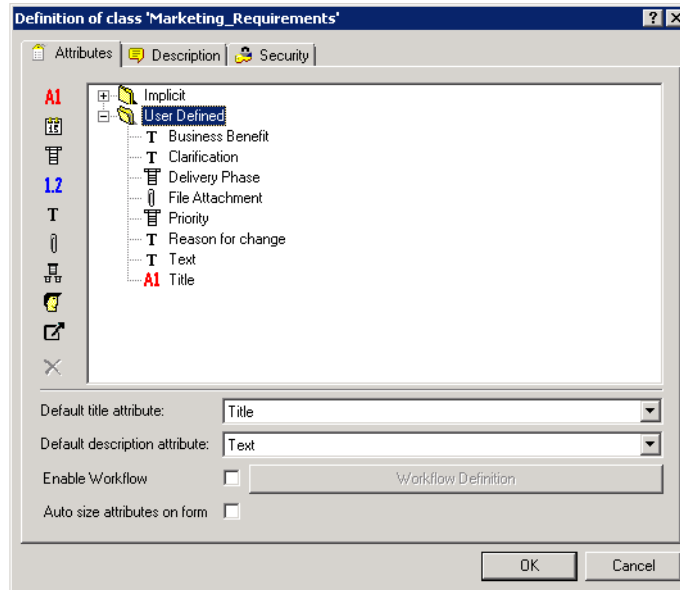
4   To commit the name change, click an empty area of the canvas.

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 "Attributes" on page 298.
Description tab	Allows to set a description to the class.
Security tab	Allows to create security profiles for the class. For details, see chapter "Security" on page 342.
Default title attribute	Allows to select the attribute which is used as a title. Only alphanumeric attributes can be selected. For details, see chapter "Alphanumeric Attribute" on page 299).
Default description attribute	Allows to select the attribute which is used for the description. Only text attributes can be selected. For details, see chapter "Text Attribute" on page 313.
Enable Workflow	If enabled, the class is using a workflow for each requirement.
Workflow Definition	Opens the Workflow Definition editor. For details, see chapter "Workflows" on page 353.
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 298.

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 298.

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 342.

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.
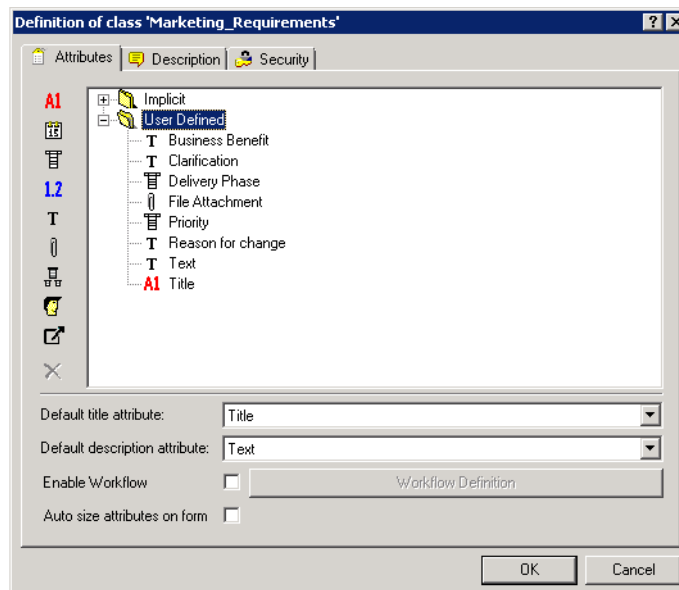
Figure 9-17. Class Definition

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 31.

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.
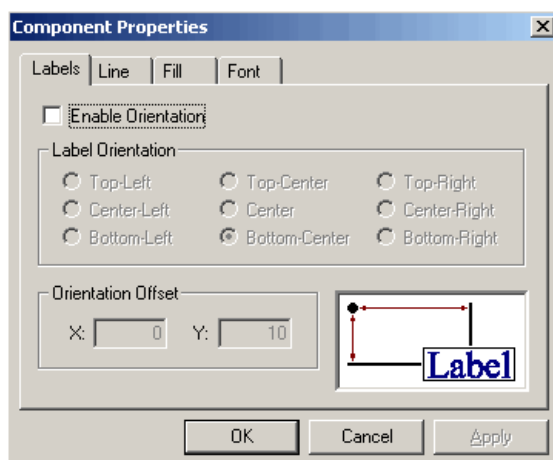
Figure 9-18. Component Properties

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 reposition 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 31.

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.
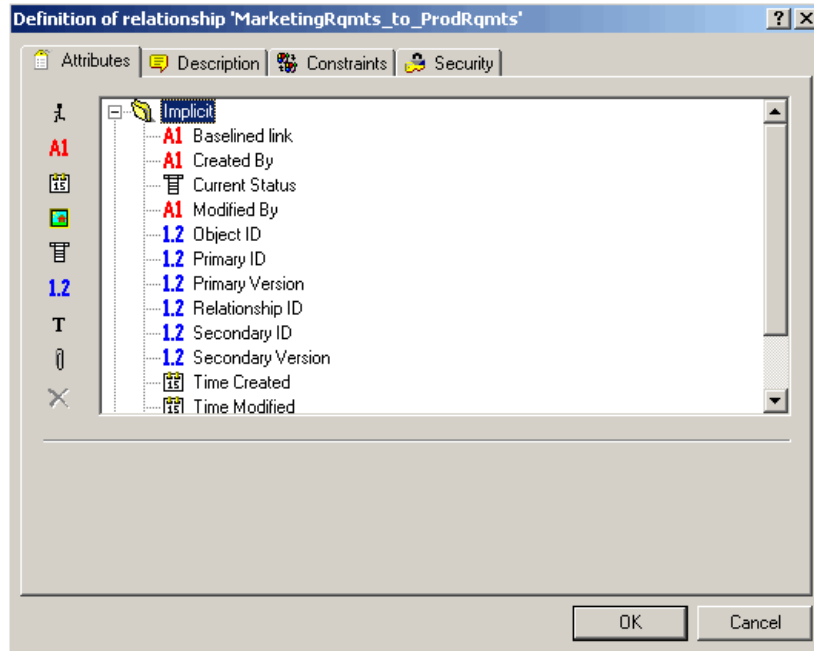
Figure 9-19. Relationship Definition

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 298.

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.

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 334.

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 **Change Raises Suspicion** in chapter "Core Tab" on page 318.
mark secondary as suspect on link deletion	When the link between the primary object and the secondary object is deleted, 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 "Core Tab" on page 318).
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 **Current** 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 **Change Raises Suspicion** in chapter "Core Tab" on page 318.
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 318).
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 **Current** 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

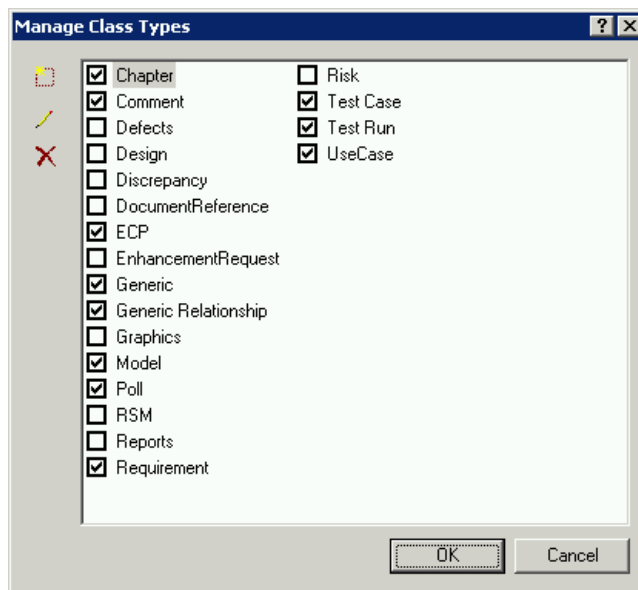For information about specifying security, see "Security" on page 342.

Class Types

This section describes how to work with class types.

Defining a Class Type

To define a class type:

1   In **Class Definition**, right-click a blank place in the grid.

2   Select **Add Class** | **Manage class types**.

The **Manage Class Types** dialog box opens.

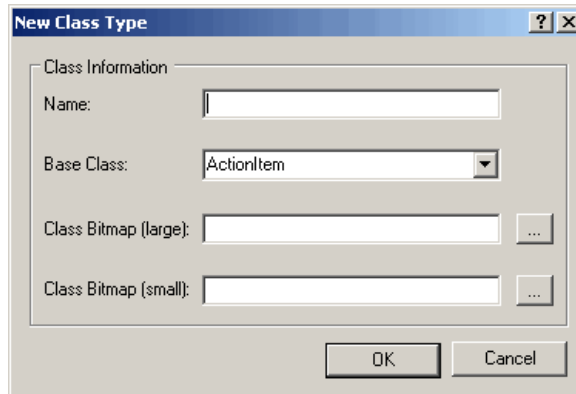***Figure 9-21. Manage Class Types***

A selected check box indicates that the class type is valid and can be added to the instance schema.

3   Click **OK**.

Adding a New Class Type

To add a new class type definition:

1   Click the **Add** button ⬜ on the **Manage Class Types** dialog box. The **New Class Type** dialog box opens.

Figure 9-22. New Class Type

2   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:

1   Select the type on the **Manage Class Types** dialog box.

2   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:

1   Select the class type on the **Manage Class Types** dialog box.

2   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 298.

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**.
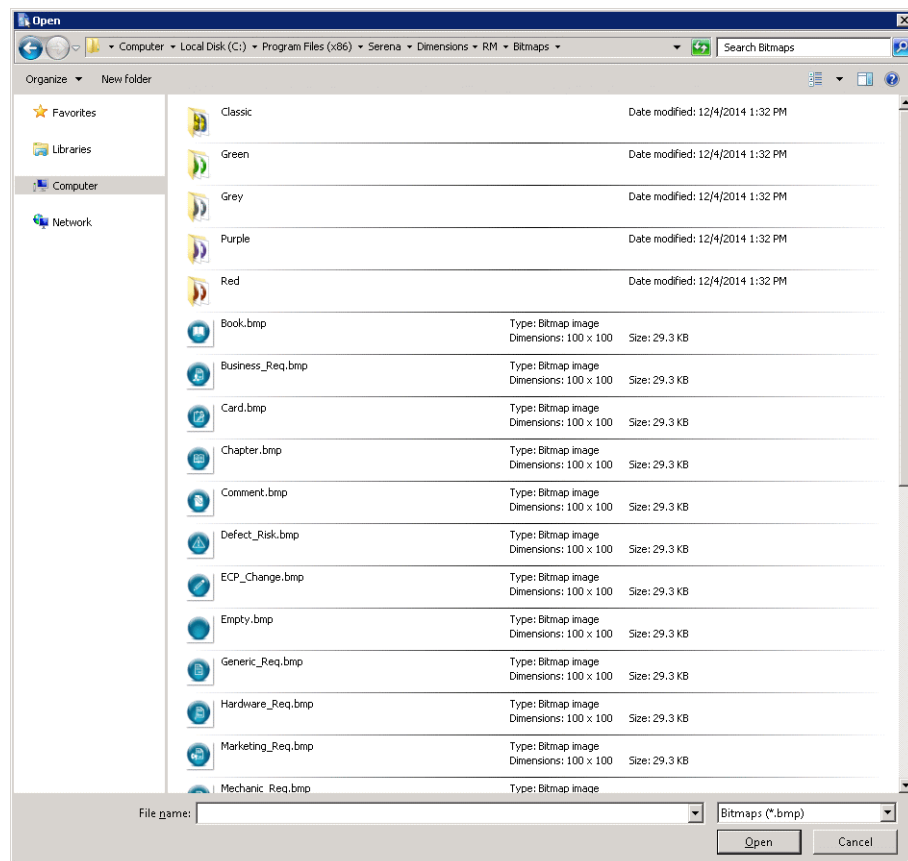
Figure 9-23. Class Type Definition Visual

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.
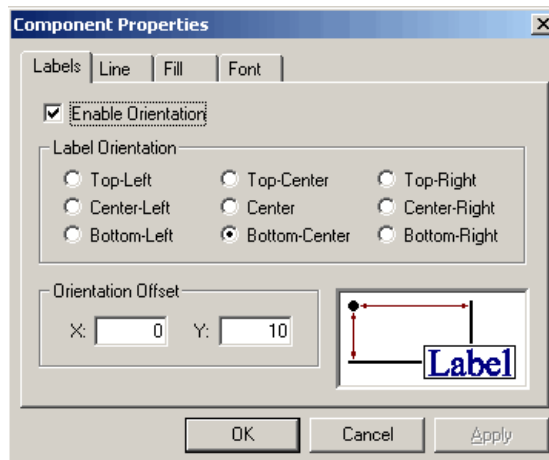
Figure 9-24. Component Properties

3   Customize the format of the label for the class type.

Security

> **NOTES** As a good general practice, Micro Focus recommends that no Dimensions RM group or user (including Administrators) ever be granted the class access rights for: REMOVE, UPDATE, and UPDATE NON_CURRENT.
>
> Update should not be granted to anyone on the system. All requirements changes should be performed with the replace function. This approach allows a fully auditable change history to be maintained and thus exposes Dimensions RM full capabilities. But this approach does require that you baseline requirements to capture the versions that you are currently capturing with the replace button. If users start using baselines and snapshots with other usage models (primarily updates and replace to version), they will be forced to create a new version just because someone else created a baseline. This may also limit the compare functions in Dimensions RM.

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.

Class Definition allows the instance administrator 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 will vary (see the appropriate table in this section for specific details about the transactions available for each resource type), but the method for defining the security profile is the same. 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 will be used.

> **NOTE** The security constraints placed on any individual entity in class definition will apply to that entity only. Use RM Manage to apply more general security policies across the entire instance.

Granting Group Access

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.
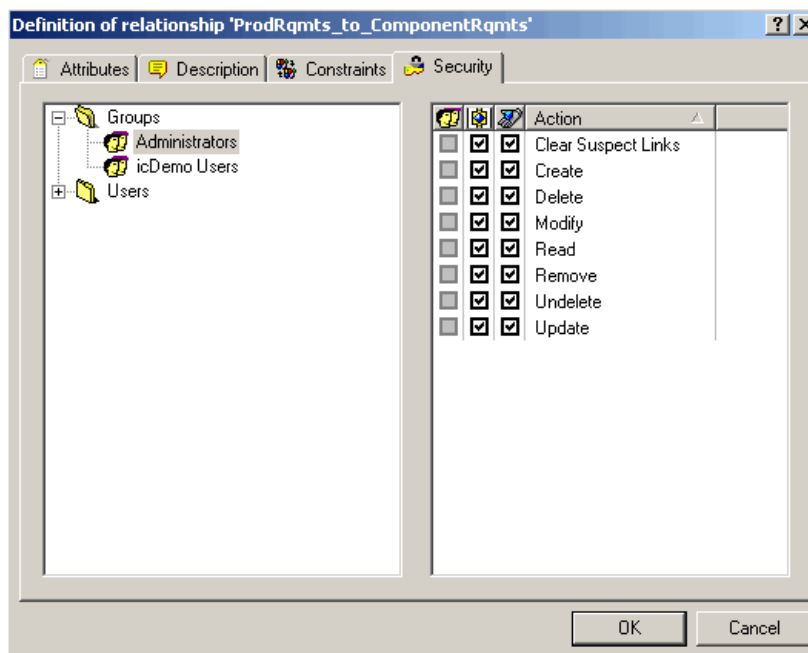
Figure 9-25. Definition of Relationship—Security Tab

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:

	Group	The **Group** setting defines if all users of a group gain access. Note that the **Group** setting cannot deny a right gained on instance level.
	Instance	The **Instance** column shows the right gained on instance level. Note that you cannot change the right here.
	Actual	The **Actual** setting defines the actual right of the group. Note that the **Actual** box is always selected if the right is gained on instance level.

Granting User Access

By default, user permissions are hidden. For information on how to show user permissions, see chapter "Showing or Hiding User Permissions" on page 211.

NOTE The user permissions feature is deprecated and will be removed in a later version.

To change the access of a user to the selected resource:

1 In **Class Definition**, right-click the class and select **Define**.

2 Click the **Security** tab.

3 Click + next to **Users**.

4 Select the user.

5 Click the required transaction to toggle the access rights. For user access rights, the user can be granted one of three access levels:

- Explicit access is indicated by a checked box ☑

- Explicit denial is indicated by an unchecked box ☐

- Inherited access is indicated by a grayed box ▣ .

6 Click **OK**.

7 Save the instance schema.

Access Rights:

🔲	**User**	The **User** setting defines if a user of a group gains access. Note that the User setting cannot deny a right gained on group or instance level.
🔲	**Group**	The **Group** column shows the right gained on group level. Note that you cannot deny a right gained on group level.
🔲	**Instance**	The **Instance** column shows the right gained on instance level. Note that you cannot change the right here.
🔲	**Actual**	The **Actual** setting defines the actual right of the group. Note that the **Actual** box is always selected if the right is gained on instance level or group level.

Order of Precedence

The use of groups and the ability to allow and disallow users from 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, an order of precedence is used by the Dimensions RM security system. The order of precedence (from highest precedence to lowest precedence) is shown in the following table.

Source of Access	Allowed Status
An individual user has been explicitly denied access to a resource or transaction.	Denied
An individual has been granted explicit access to a resource or transaction.	Allowed
An individual has been granted access to a resource or transaction through membership in a group that has been granted access.	Allowed
An individual has been explicitly denied access to an entire category of resources through default access rights.	Denied

Source of Access	Allowed Status
An individual has been explicitly allowed access to an entire category of resources through default access rights.	Allowed
An individual has been allowed access to an entire category of resources through membership in a group that has been granted access rights to a category of resources.	Allowed
No entries exist specifying access rights for the individual or any groups of which the individual is a member in the access rights list.	Denied

Valid Transactions

The tables in the following sections list the valid transactions for classes, relationships, and source documents.

Valid Transactions 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. **NOTE:** 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 **Delete** right is required on the **Chapter** class if users are to delete chapters. Note that before Dimensions RM 12.6.1, the **Remove** 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.

Transaction	Description
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

To save the instance schema, select **File** | **Save** or click the **Save** 💾 button.

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

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.
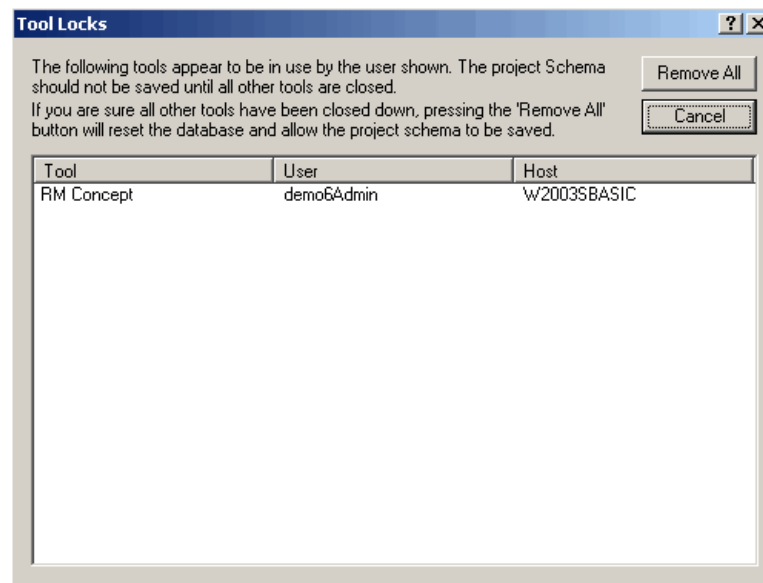
Figure 9-26. Tool Locks

You can cancel the save operation until other users have finished working, or you can click **Remove All** to remove the tool locks. This allows you to save the instance schema, but it may adversely effect the operations being performed by the other users.

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 to Another Instance

You can directly deploy an instance schema to another instance. This may be of use when transferring a schema from a development system to the production system. Note that the default installation allows to deploy to any instance within the same database only. If you wish to deploy to another database (e.g. on a different machine), the database connection information of the target machine must be present in the tnsnames.ora file of your machine running the Class Definition tool.

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. This also removes the data of these classes.

■ If security permissions are copied, the security permissions for groups on the target are overwritten. User permissions and category permissions are not copied.

To deploy the instance schema to another instance:

1 In **Class Definition**, 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**.

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 333.

2 Specify the **Clear Suspect Links** action for each user and group that should have permission to clear suspect links. For more information, see .

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 9-27. 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

Element	Meaning
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 "-"
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 "RRRR Date Format Elements" on page 352. **NOTE:** This is the preferred format for 4-digit years.
SSSSS	Seconds past midnight (0-86399)

Element	Meaning
YEAR SYEAR	Year spelled out; "S" prefixes BC dates with "-"
YYYY SYYYY	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.
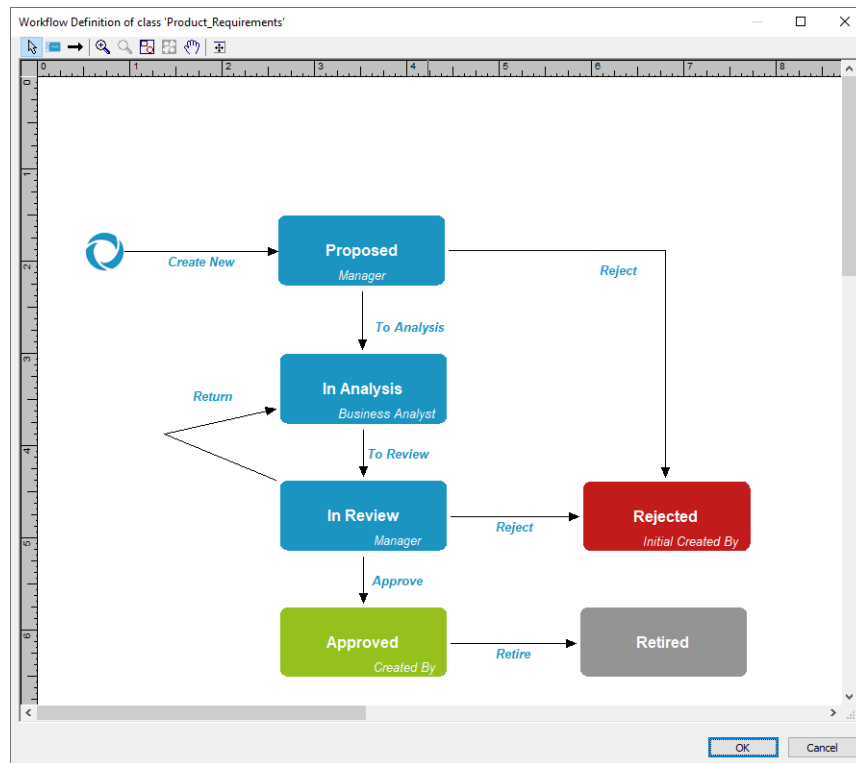
Figure 9-28. Workflow for class Product_Requirements

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	Display the attribute if its parent section is also displayed. **NOTE** If you choose to hide (not display) attributes on selected workflow forms, please test the display. 1 Check to ensure that the modified display will not confuse users. 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.
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 .

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. **NOTE** 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.

Attribute Constraint Settings

To change the attribute constraint settings, select the **Attribute Constraints** tab. By creating or modifying attribute constraints you define under which conditions the transition can be executed.
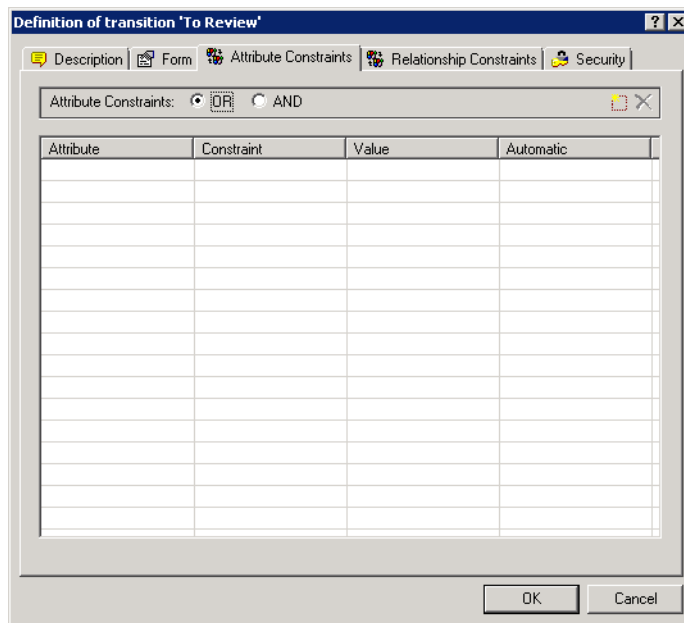
Figure 9-29. Attribute Constraint Settings dialog

NOTE Attribute Constraints are checked when clicking the associated button.

To add attribute constraints:

1   Click **OR** or **AND** in the **Attribute 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 attribute constraint:

1   Click the **New Constraint** button in the **Attribute Constraints** area.

A new row is added to the table and the **Attribute** cell is populated. If needed, click on the **Attribute** cell to select a different attribute from a drop-down menu.

2   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`.

- **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.
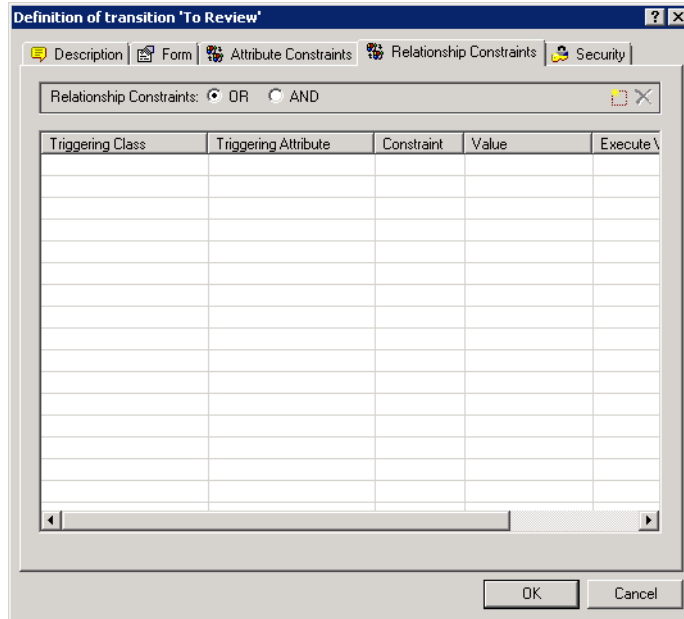
Figure 9-30. Relationship Constraint Settings dialog

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 292.

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 342.

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 317.

9   Add a workflow to the *WorkFlow_Container* class as described in chapter"Creating or Editing a Workflow" on page 354.

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 292).

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 292).

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 ![icon] 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 30.

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 ![icon] 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 31.

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 ![icon] in the toolbar or by selecting **Save** from the **File** menu.

Chapter 10
Configuring Tomcat

Working with Secure Socket Layers

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

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

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

Configuration Overview

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

For details on importing the certificate to IIS, see chapter "Importing a PFX Certificate into Microsoft IIS" on page 450.

If you are not using IIS, see chapter "Importing a PFX Certificate into Windows" on page 450.

> **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 454 or

- "Exporting Certificates to CER Format from IIS" on page 453.

- **PFX Format:**

  - "Exporting Certificates to PFX Format from the Management Console" on page 454 or

  - "Exporting Certificates to PFX Format from IIS" on page 455.

> **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 459.

To import the certificate, do the following:

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

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

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

   c Click ■.

2 Open a command prompt.

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

> **NOTE**
>
> - Replace *`RM_Install`* with the path to the Dimensions RM directory, e.g. *C:\Program Files\Micro Focus\Dimensions 12.10*.
>
> - Replace ***#.#.#.#*** with the Common Tools version number, e.g. *1.8.6.0*.
>
> - Replace ***#.#*** with the Java version number, e.g. 11.0.
>
> The complete set command may look like this:
>
> `set path=%path%;"`*`C:\Program Files\Micro Focus\Dimensions`*` 12.10\Comm on Tools `*`1.8.6.0`*`\jre\`*`11.0`*`\bin"`

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

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

> **NOTE**
>
> ■ Replace *RM_Install* with the path to the Dimensions directory, e.g.
> *C:\Program Files\Micro Focus\Dimensions 12.10*.
>
> ■ Replace **#.#.#.#** with the Common Tools version number, e.g. 1.8.6.0.
>
> ■ Replace **#.#** with the Tomcat version number, e.g. 9.0.
>
> A complete path may look like this:
>
> *C:\Program Files\Micro Focus\Dimensions 12.10*\Common Tools *1.8.6.0*\
> tomcat*9.0*\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 459.
>
> ■ 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 378.

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

Modifying the Server.xml File

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

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

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

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

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

    c Click ■.

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

> **NOTE**
>
> ■ Replace *RM_Install* with the path to the Dimensions directory,e.g. *C:\Program Files\Micro Focus\Dimensions 12.10*.
>
> ■ Replace **#.#.#.#** with the Common Tools version number, e.g. 1.8.6.0.
>
> ■ Replace **#.#** with the Tomcat version number, e.g. 9.0.
>
> A complete path may look like this:
>
> *C:\Program Files\Micro Focus\Dimensions* 12.10\Common Tools *1.8.6.0*\ tomcat*9.0*\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 **Micro Focus Common Tomcat** service. To start the service, follow these steps:

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

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

   c Click ▶ .

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

Updating the Dimensions RM Server Certificate

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

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

- **CER Format:**

   • "Exporting Certificates to CER Format from the Management Console" on page 452 or

   • "Exporting Certificates to CER Format from IIS" on page 453.

- **PFX Format:**

   • "Exporting Certificates to PFX Format from the Management Console" on page 454 or

   • "Exporting Certificates to PFX Format from IIS" on page 455.

> **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 459.

To update the certificate, do the following:

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

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

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

    c Click ■

2 Open a command prompt.

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

> **NOTE**
>
> - Replace *RM_Install* with the path to the Dimensions RM directory, e.g. *C:\Program Files\Micro Focus\Dimensions 12.10*.
>
> - Replace **#.#.#.#** with the Common Tools version number, e.g. *1.8.6.0*.
>
> - Replace **#.#** with the Java version number, e.g. 11.0.
>
> The complete set command may look like this:
>
> `set path=%path%;"`*`C:\Program Files\Micro Focus\Dimensions`*` 12.10\Common Tools `*`1.8.6.0`*`\jre\`*`11.0`*`\bin"`

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

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

> **NOTE**
>
> - Replace *RM_Install* with the path to the Dimensions directory, e.g. *C:\Program Files\Micro Focus\Dimensions 12.10*.
>
> - Replace **#.#.#.#** with the Common Tools version number, e.g. 1.8.6.0.
>
> - Replace **#.#** with the Tomcat version number, e.g. 9.0.
>
> A complete path may look like this:
>
> *C:\Program Files\Micro Focus\Dimensions 12.10*\Common Tools *1.8.6.0*\tomcat*9.0*\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\Micro Focus\Dimensions` 12.10`\Common Tools` 1.8.6.0`\tomcat\9.0`). 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\Micro Focus\Dimensions 12.10\Comm
> on Tools 1.8.6.0\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 459.

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

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

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

    c Click

Updating SSO Certificates

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

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

■ Federation Server certificate (*fedsrv.cer*)

■ STS certificate (*sts.cer*)

■ SSO Gatekeeper certificate (*gatekeeper.cer*)

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

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

To update the certificates, execute these steps:

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

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

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

   c Click ▮

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

> **NOTE**
>
> ■ Replace *RM_Install* with the path to the Dimensions RM directory, e.g. *C:\Program Files\Micro Focus\Dimensions 12.10*.
>
> ■ Replace ***#.#.#.#*** with the Common Tools version number, e.g. *1.8.6.0*.
>
> ■ Replace ***#.#*** with the Java version number, e.g. 11.0.
>
> The complete set command may look like this:
>
> `set path=%path%;"`*C:\Program Files\Micro Focus\Dimensions* `12.10\Comm on Tools `*1.8.6.0*`\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\Micro Focus\Dimensions 12.10*.
>
> ■ Replace **#.#.#.#** with the Common Tools version number, e.g. 1.8.6.0.
>
> ■ Replace **#.#** with the Tomcat version number, e.g. 9.0.
>
> A complete path may look like this:
>
> *C:\Program Files\Micro Focus\Dimensions 12.10*\Common Tools *1.8.6.0*\tomcat*9.0*\alfssogatekeeper\conf

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

 c Click ▶

Importing Certificates on the Client

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

Importing Certificates with Internet Explorer / Edge / Chrome

To import a certificate, execute these steps:

1   Open a command prompt.

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

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

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

5   Click **Add**.

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

    a   Select **Computer account**.

    b   Click **Next**.

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

    d   Click **Finish**.

7   Click **OK**.

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

9   Expand **Trusted Root Certification Authorities**.

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

11   Click **Next**.

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

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

14   Click **Next**.

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

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

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

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

16   Click **Next**.

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

18   Restart Internet Explorer, Edge, or Chrome respectively.

Importing Certificates with Firefox

To import a certificate, execute these steps:

1 Start Firefox if it is not already running.

2 Click ≡ to open the settings menu.

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

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

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

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

7 Select the **Authorities** tab.

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

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

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

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

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

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

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

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

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

14 Restart Firefox.

Configuring Secure Cookies

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

NOTE

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

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

To configure secure cookies, do the following:

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

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

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

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

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

5 Save the file.

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

Configuring HTTP Strict Transport Security and Anti-Clickjacking

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

Anti-Clickjacking prevents external websites to overlay Dimensions RM elements (e.g.
buttons). This ensures that if a user clicks on a Dimensions RM element an element from
a different website can't "catch" its click.

To configure HTTP Strict Transport Security, do the following:

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

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

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

4 Remove the following content:

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

5 Add the following content:

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

```
</init-param>
<init-param>
<param-name>antiClickJackingOption</param-name>
<param-value>SAMEORIGIN</param-value>
</init-param>
</filter>
<filter-mapping>
<filter-name>httpHeaderSecurity</filter-name>
<url-pattern>/*</url-pattern>
<dispatcher>REQUEST</dispatcher>
</filter-mapping>
```

> **NOTE** For further information on the options and defaults, see the comment before the `<filter>` tag in your web.xml file.

6   Save the file.

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

Configuring Azure Login for the Login Page

To configure Azure login, do the following:

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

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

3   Search for the **primary_login** setting:
```
<param-name>primary_login</param-name>
```

4   Locate the associated **param-value** node and change its value as desired:

- **azuresso:** Log in using Azure

- **internal:** Log in using Dimensions RM default log in handling

The following code sample shows the login setting for Azure:
```
<init-param>
  <param-name>primary_login</param-name>
  <param-value>azuresso</param-value>
</init-param>
```

5   Save the file.

6   Start the **Micro Focus 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 1.8.6.0\tomcat\9.0\bin

> **NOTE**
>
> Replace *RM_Install* with the path to the Dimensions directory, e.g.
> *C:\Program Files\Micro Focus\Dimensions 12.10*.

2 Create a copy of the file `tomcat8w.exe`.

3 Rename the copy to `MicroFocusTomcatw.exe`.

Removing the Certificate Update Menu

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

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

> **NOTE** Users cannot work with Dimensions RM or any other web application on the
> same Tomcat server for the time of your changes.

2 In Windows Explorer, navigate to the following path:
   RM_Install\Common Tools 1.8.6.0\tomcat\9.0\webapps\rtmBrowser\rm\fra
   me\panels\top

> **NOTE** Replace *RM_Install* with the path to the Dimensions directory, e.g.
> *C:\Program Files\Micro Focus\Dimensions 12.10*.

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 1.8.6.0\tomcat\9.0\work

NOTE Replace *RM_Install* with the path to the Dimensions directory, e.g. *C:\Program Files\Micro Focus\Dimensions 12.10*.

8 Delete the Catalina folder.

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

Chapter 11
RM Import

What is RM Import?

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 411.

> **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** | **Micro Focus** | **Dimensions RM *version*** | **RM Import**.

  - Double-click the RM Import shortcut on your desktop.

■ The **RM Import login** dialog box opens.
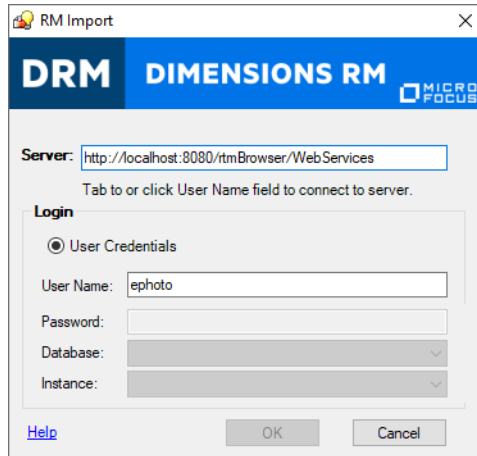
Figure 11-1. Login Dialog

■ 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.

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)
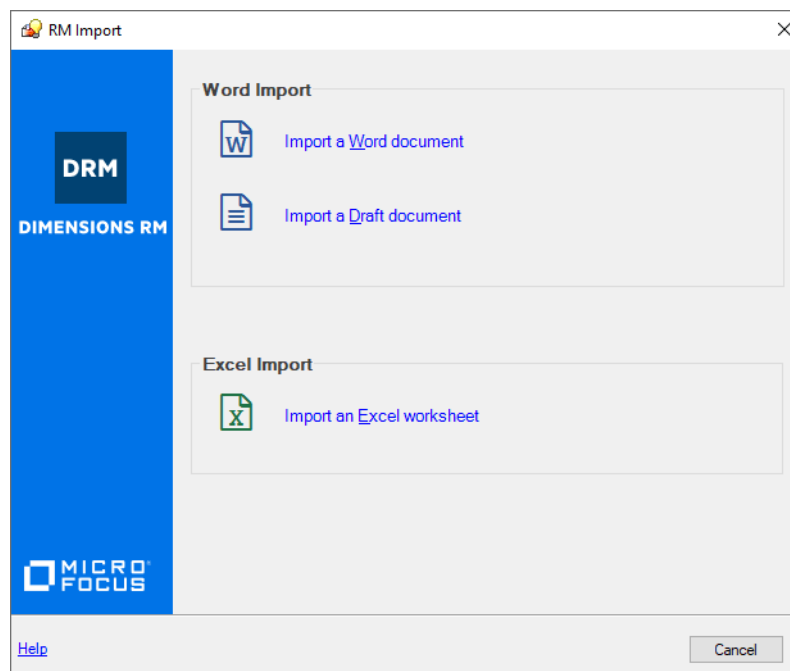
Figure 11-2. Import File Format Dialog

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.
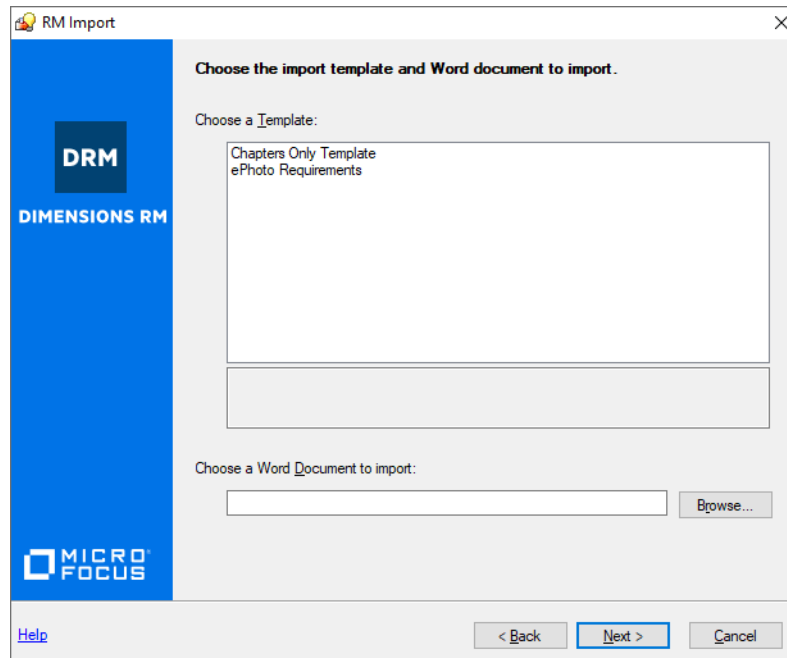
Figure 11-3. Template and Word Document Dialog

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).

■   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.
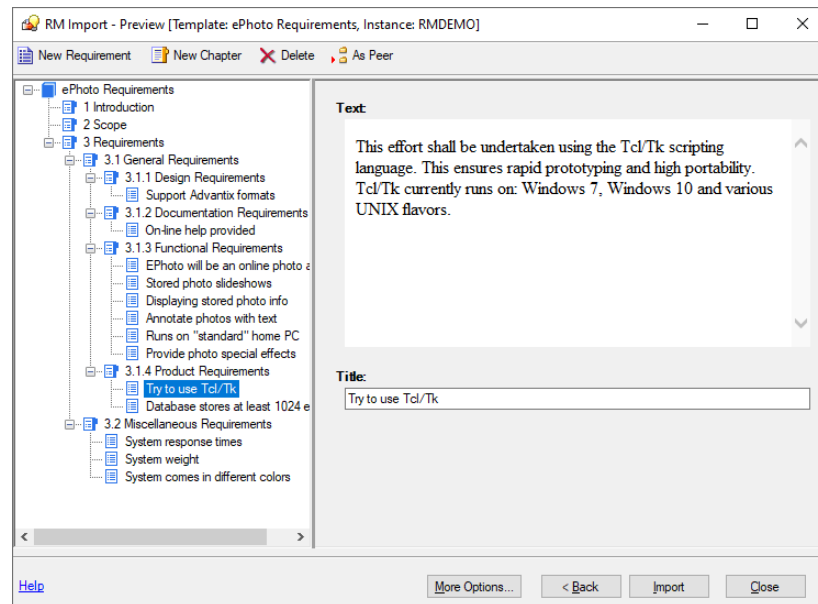
Figure 11-4. Preview Dialog

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 Micro Focus

    - 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.
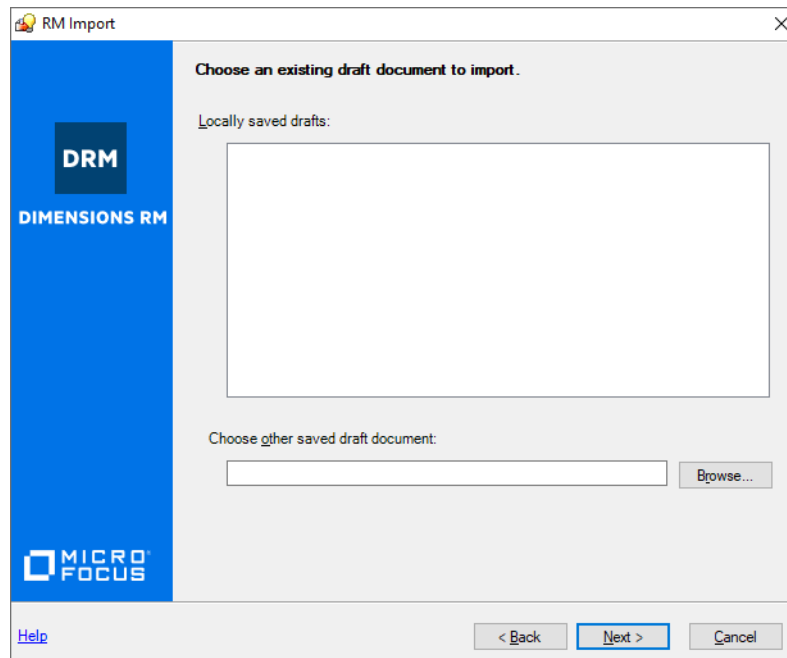
Figure 11-5. Select Draft Requirements Document Dialog

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 401).

■   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
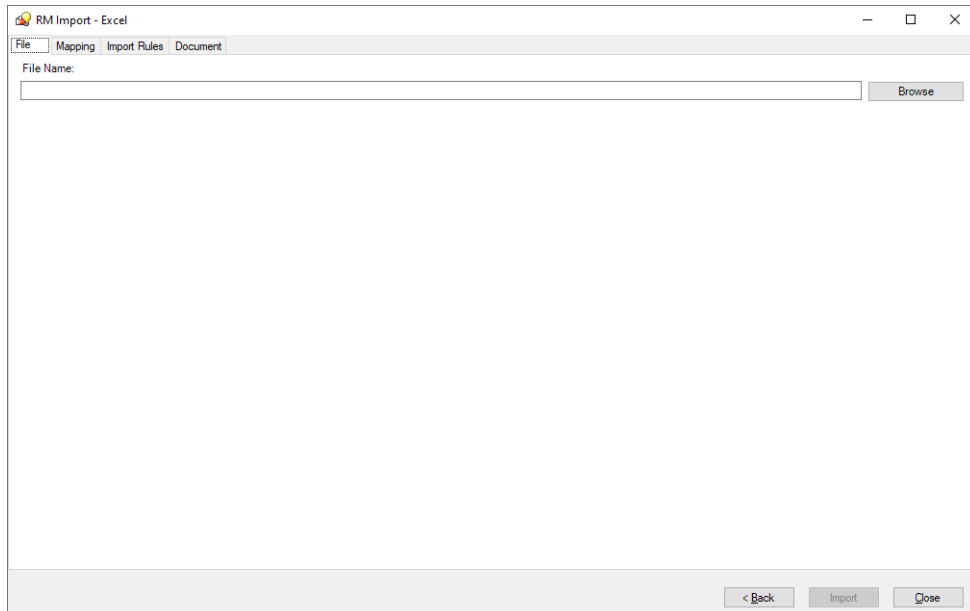
Figure 11-6. Select Excel File Dialog

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.
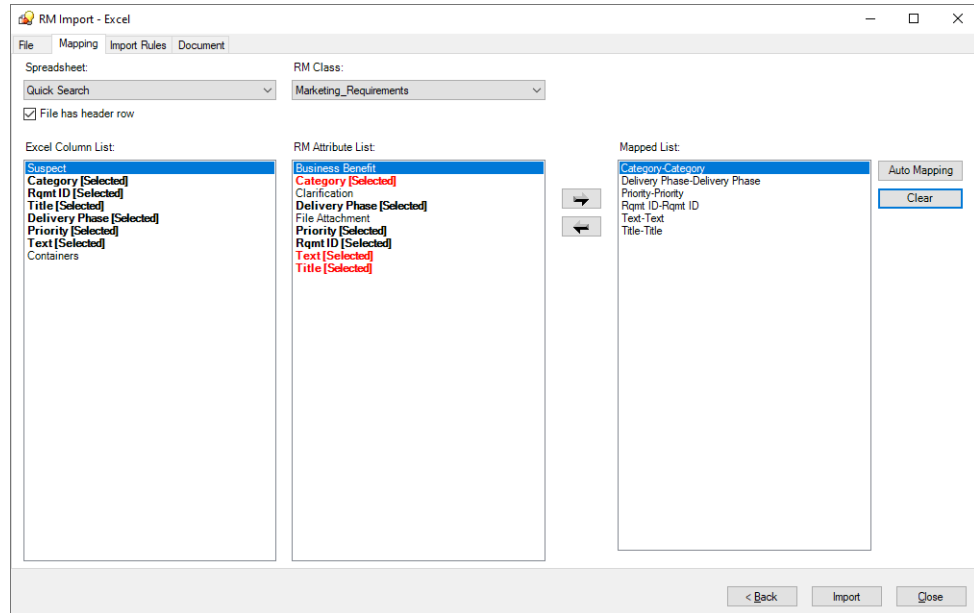
Figure 11-7. Mapping Excel columns to RM Attributes Dialog

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]**.

Mapped List	Contains the mapped Excel columns and attributes.
➡	Adds a mapping to the **Mapped List** box. To add a mapping, select one entry in the **Excel Column List** box and one entry in the **RM Attribute List** box.
⬅	Removes the selected mapping from the **Mapped List** box.
Auto Mapping	Maps all entries with identical names in **Excel Column List** box and **RM Attribute List** box.
Clear	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.
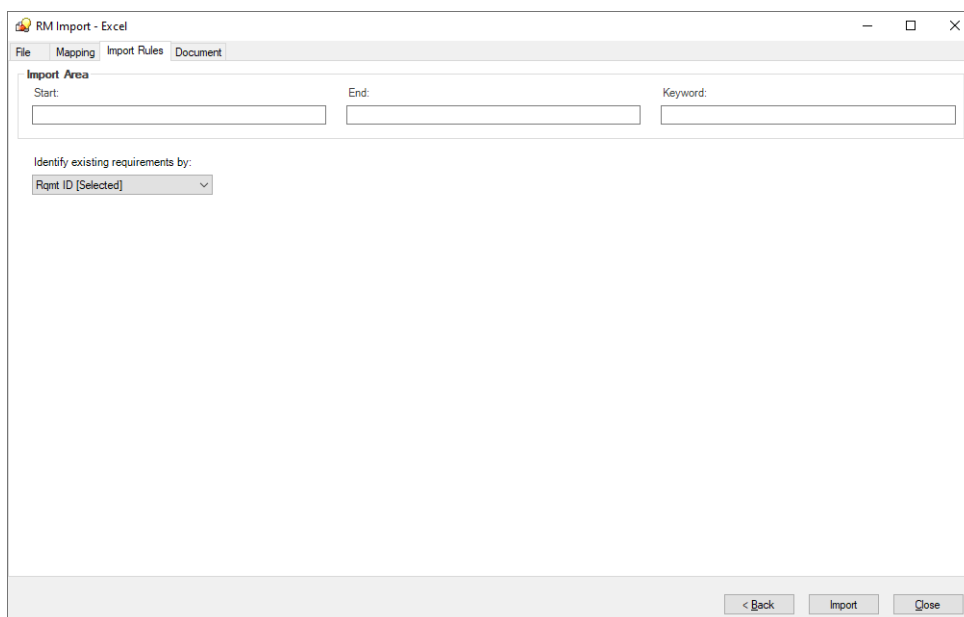
Figure 11-8. Import Rules Dialog

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 it's 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.
<u>Example</u>s:

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

RM Import Designer

What is RM Import Designer?

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.

- 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.

For more information about RM Import, see the chapter "RM Import" on page 395. 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 313.

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** | **Micro Focus** | **Dimensions RM** *version* | **RM Import Designer**.

- Double-click the RM Import Designer shortcut on your desktop.

The **RM Import Designer login** dialog box opens.
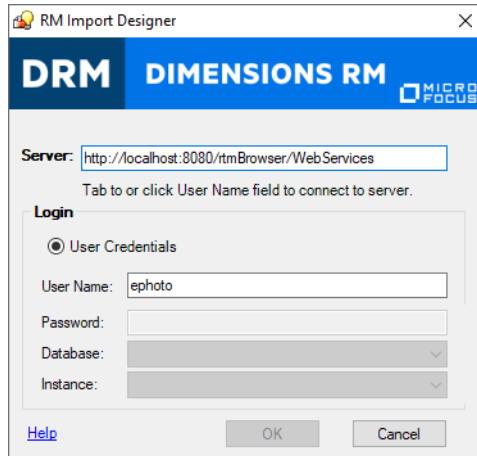
Figure 12-1. Login Dialog

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/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.

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.
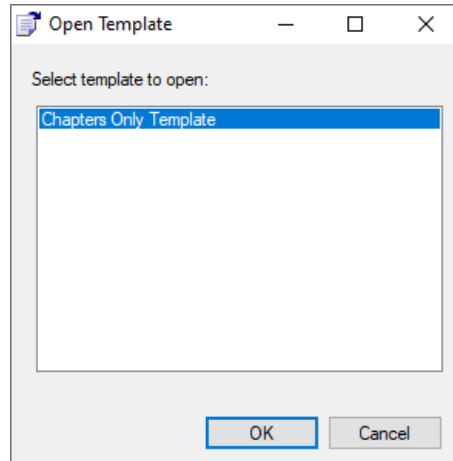
Figure 12-2. Open Template

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.
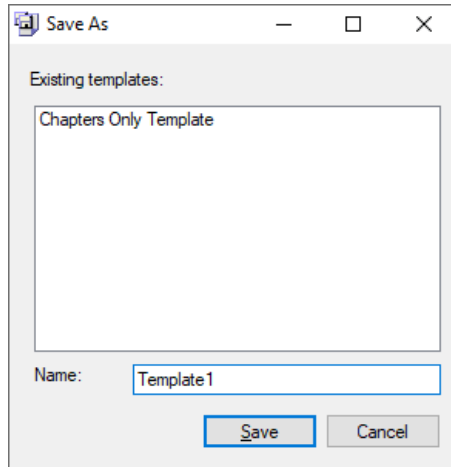
Figure 12-3. Save As

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.
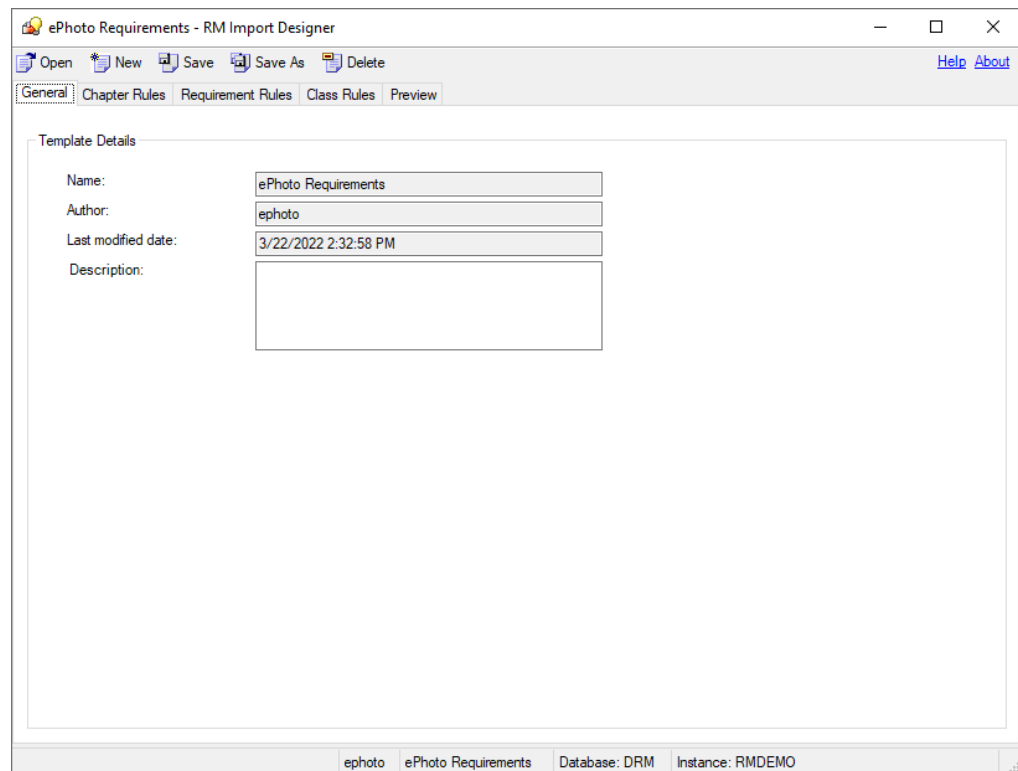
Figure 12-4. General Tab

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.
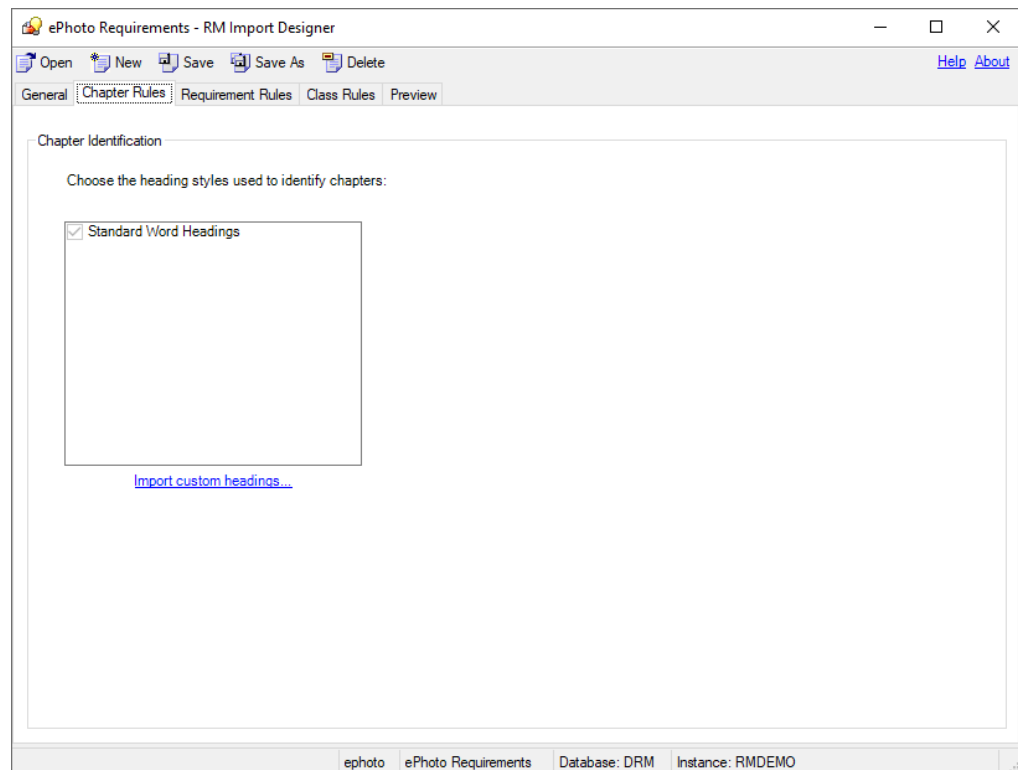
Figure 12-5. Chapter Rules Tab

> **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.
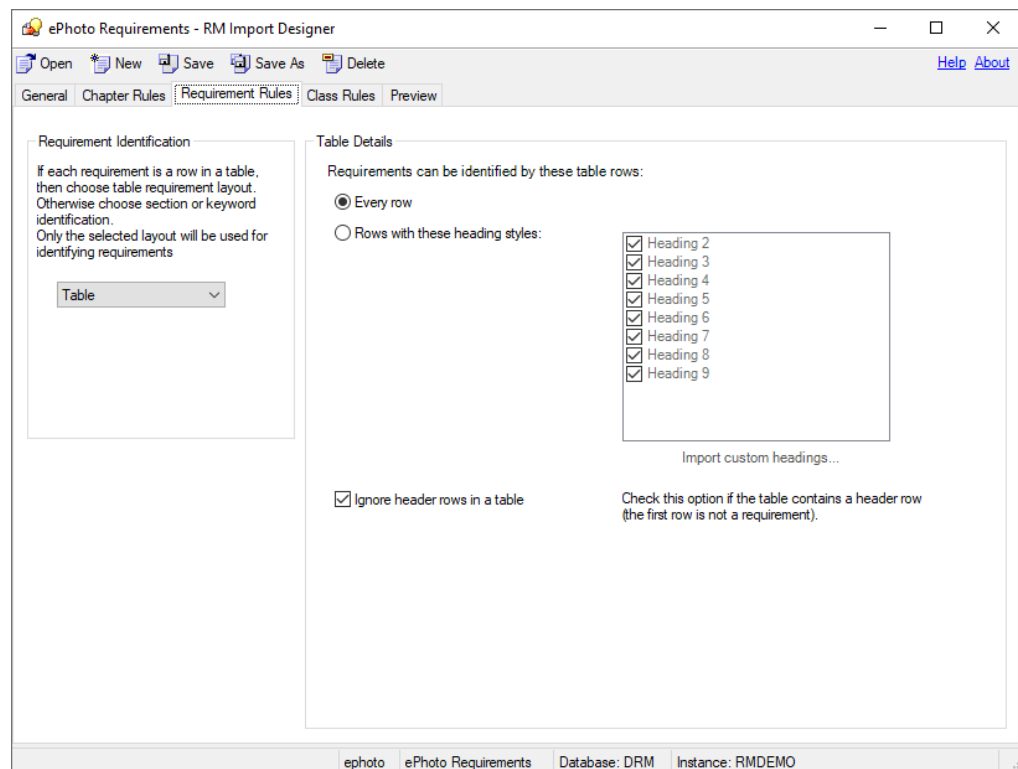
Figure 12-6. Requirement Rules Tab—Table Layout

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 **Import custom headings**, 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. **NOTE:** If you imported custom headings on the **Chapter Rules** 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.
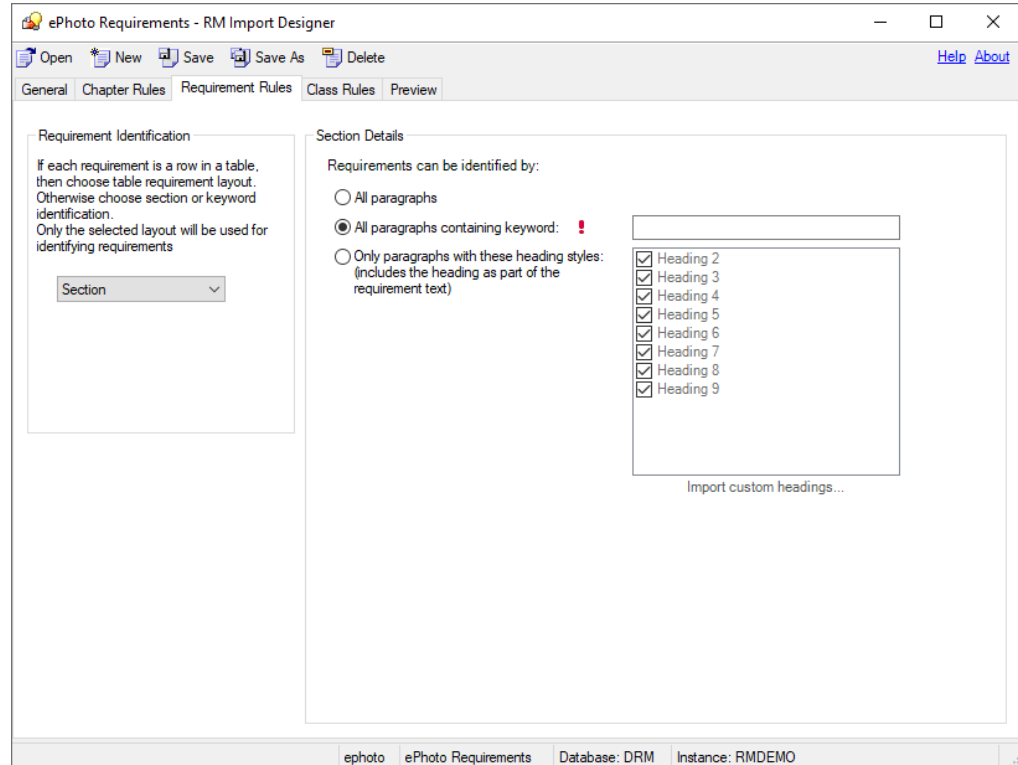
Figure 12-7. Requirement Tab—Section Option

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	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. *Shall, will,* and *must* 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 "Word Regular Expressions" on page 437. **NOTE:** When there is information between two paragraphs that contain keywords, that information is captured into the first requirement. 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. To perform a customized search, use a regular expression.
Only paragraphs with these heading styles...	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. If you want to include custom headings, click **Load custom headings** 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. **NOTE:** If you imported custom headings on the **Chapter Rules** tab, this list is automatically populated with the headings from the document you specified there.

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.
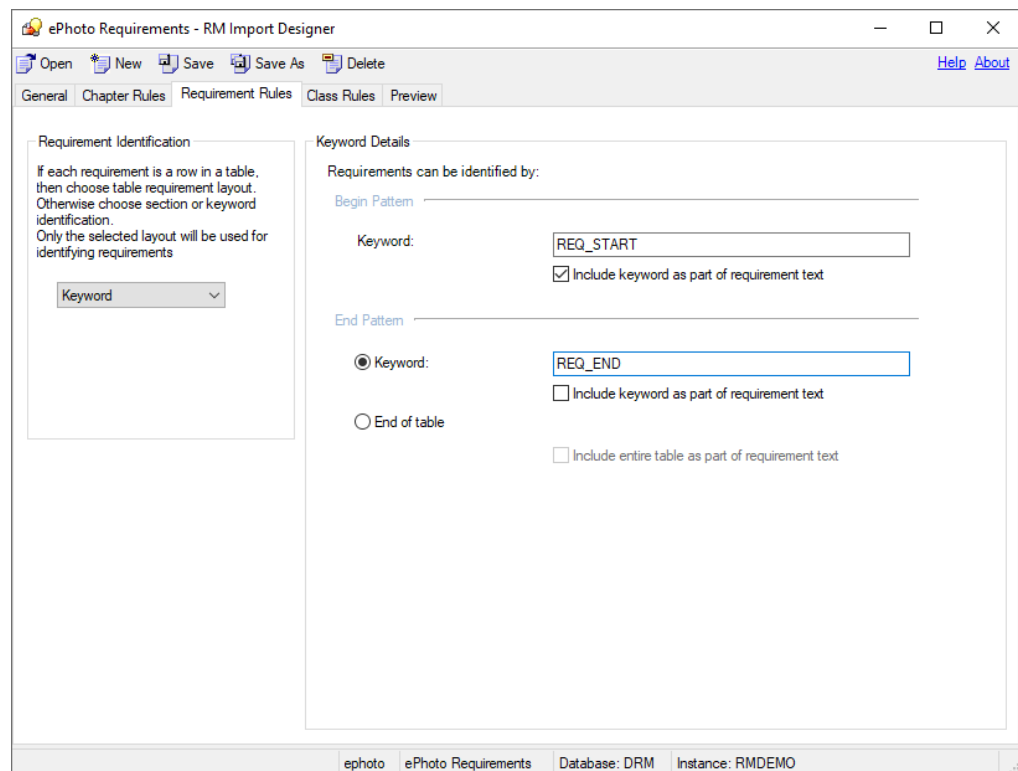
Figure 12-8. Requirement Tab—Keyword Option

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 437.

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 313.

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.
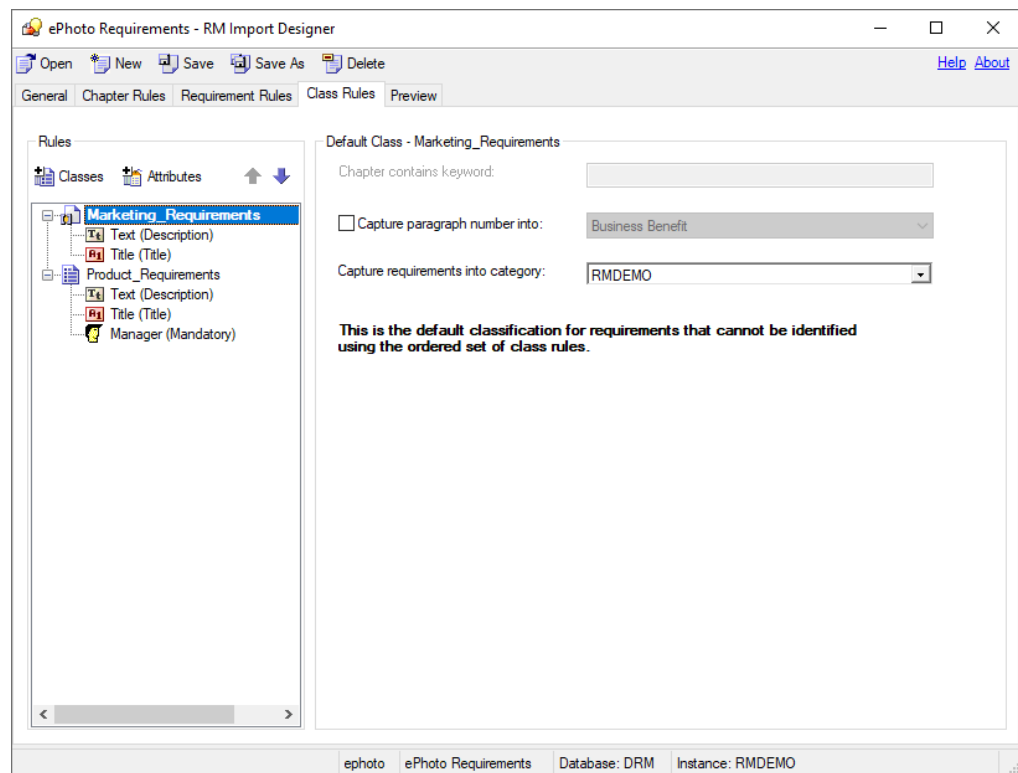
Figure 12-9. Class Rules Tab—Default Class
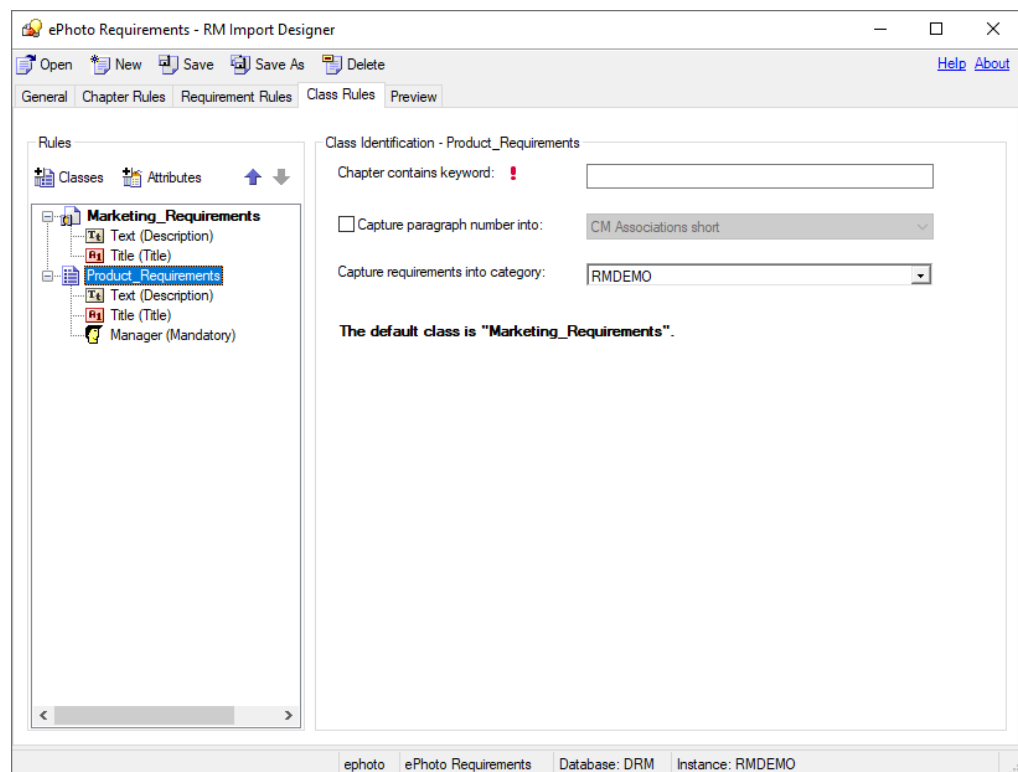
Figure 12-10. Class Rules Tab—Non-Default Class

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.
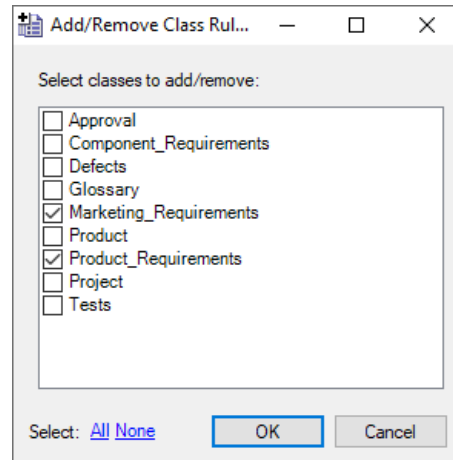
Figure 12-11. Add/Remove Class Rules

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 437.

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.
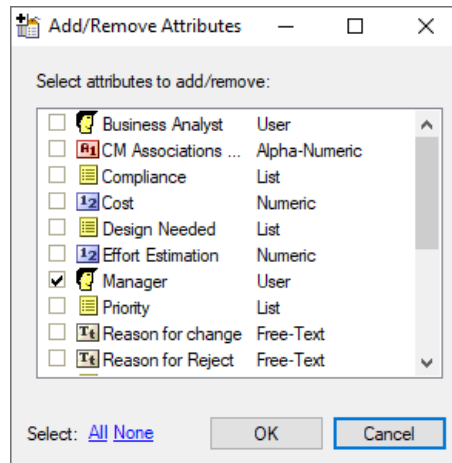
Figure 12-12. Add/Remove Attributes

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:
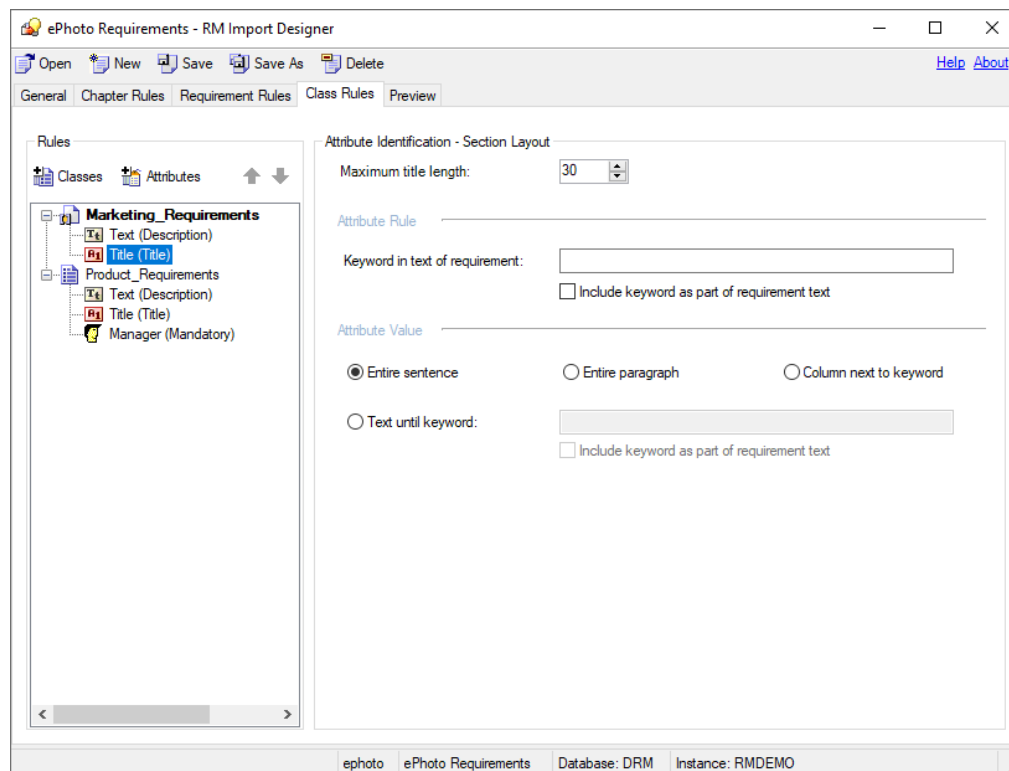
Figure 12-13. Class Rules Tab—Section or Keyword Option—Alphanumeric Attributes

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 437.

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. **NOTE:** This does not pertain to the Table option.
Text until keyword	The text up to the specified keyword is the attribute value. Select the **Include keyword as part of requirement** 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:
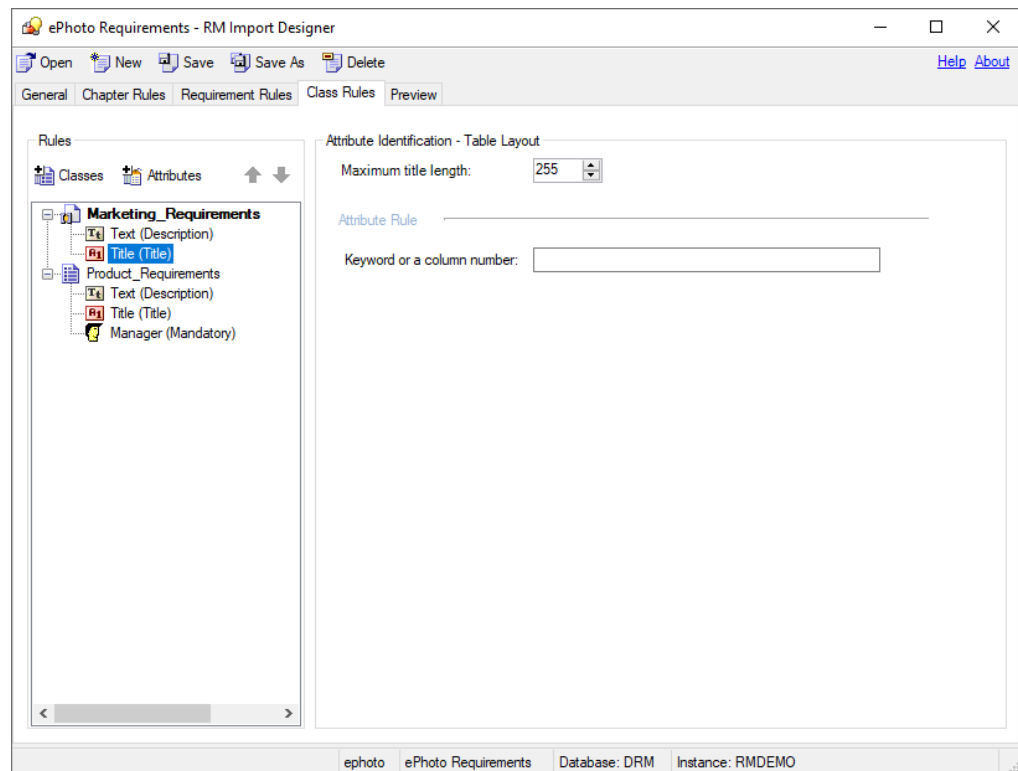
Figure 12-14. Class Rules Tab—Table Option—Alphanumeric Attributes

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, `High`). 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:
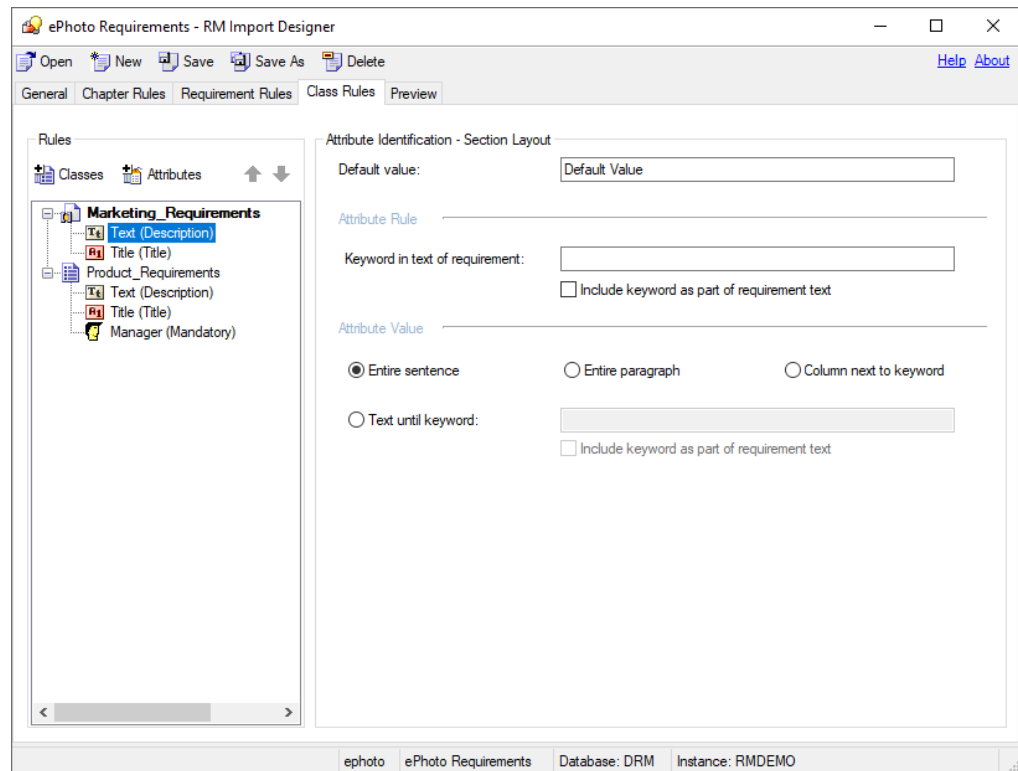
Figure 12-15. Class Rules Tab—Section or Keyword Option—Text or Numeric Attributes

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 437.

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. **NOTE:** This does not pertain to the Table option.
Text until keyword	The text up to the specified keyword is the attribute value. Select the **Include keyword** 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:
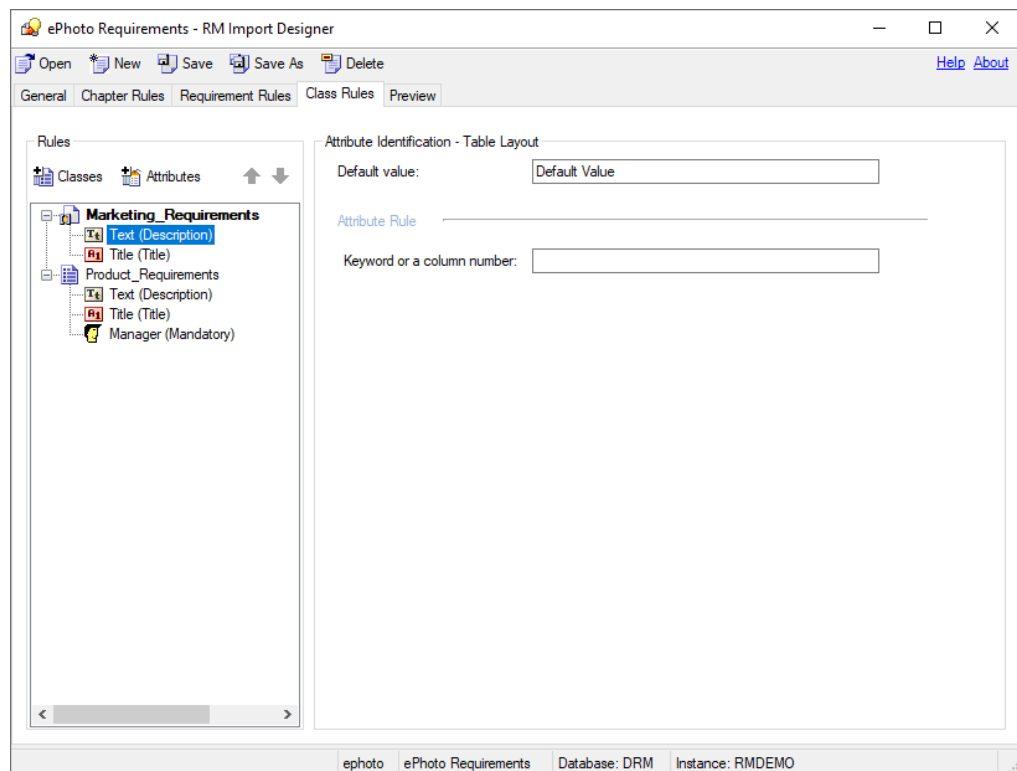
Figure 12-16. Class Rules Tab—Table Layout—Text or Numeric Attributes

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 437.

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:
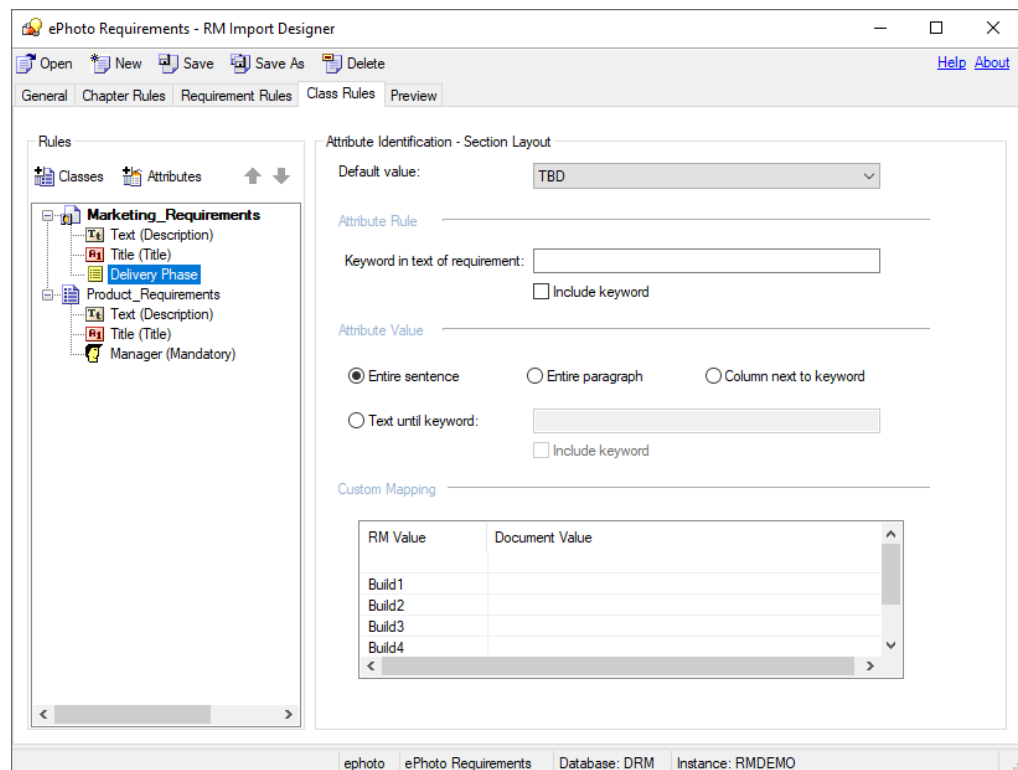
Figure 12-17. Class Tab—Section or Keyword Layout—List or User Attributes

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 437.

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. **NOTE:** This does not pertain to the Table option.
Text until keyword	The text up to the specified keyword is the attribute value. Select the **Include keyword** 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:
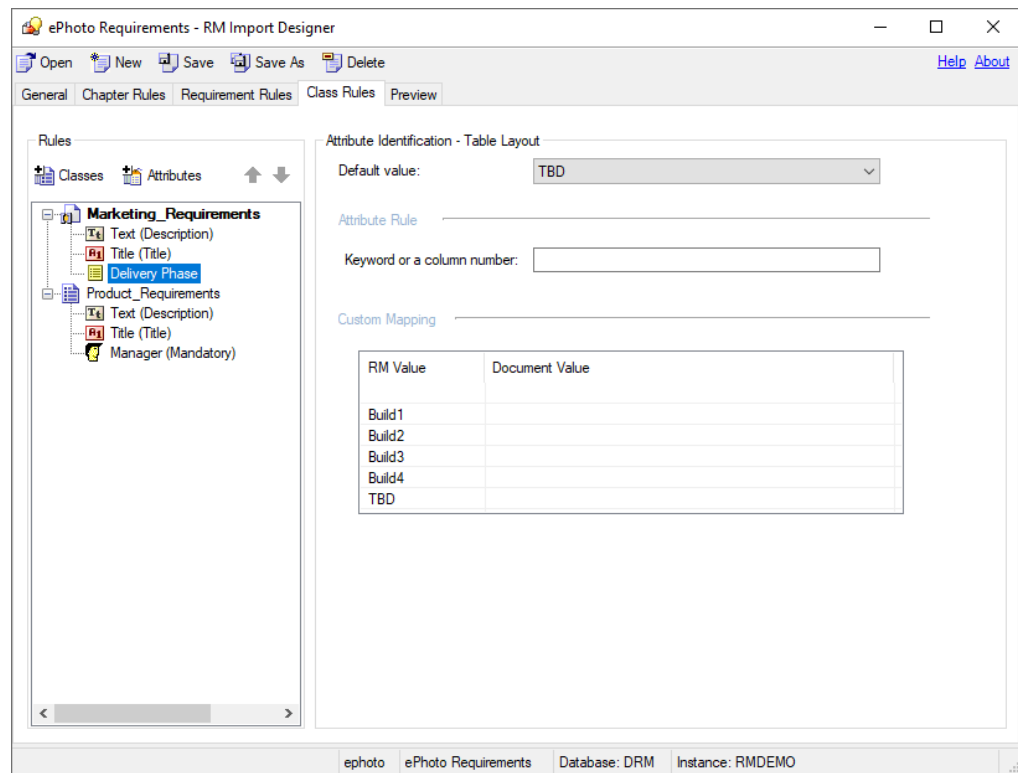
Figure 12-18. Class Rules Tab—Table Layout—List or User Attributes

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 437.

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.
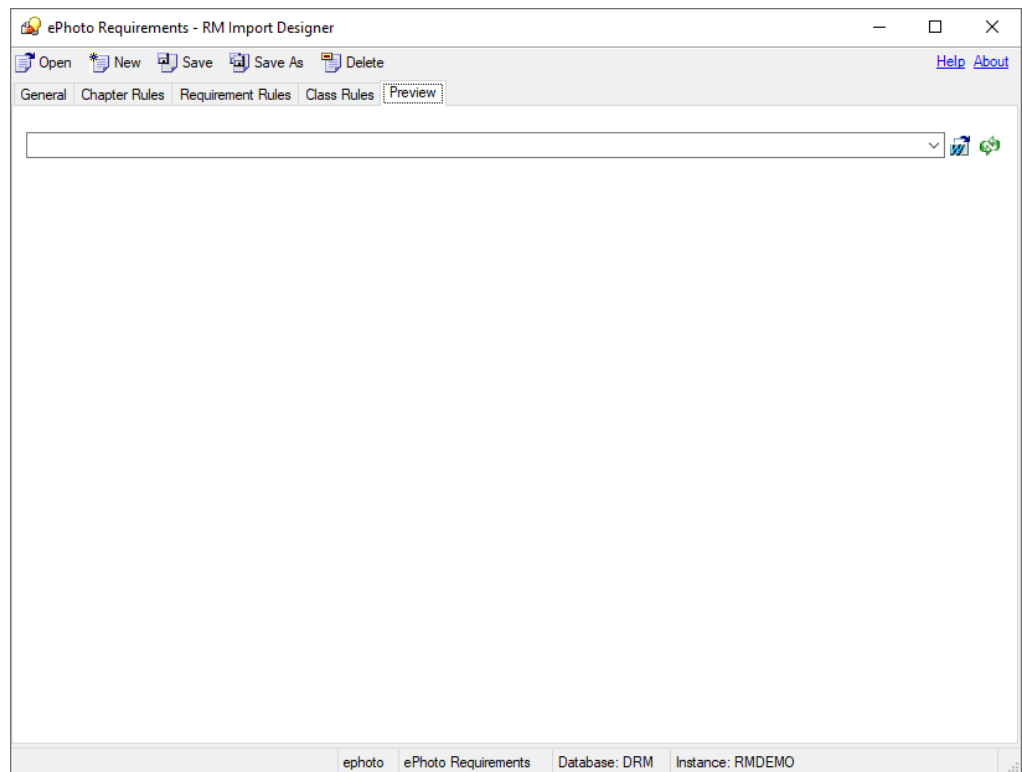
Figure 12-19. Empty Preview Tab

2   Do one of the following:

- Click the **Select a document to load** button [icon]. The **Open** dialog box opens. Select the document you want to preview and click **Open**.

- Click the **Load the currently selected document** button [icon]. 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.
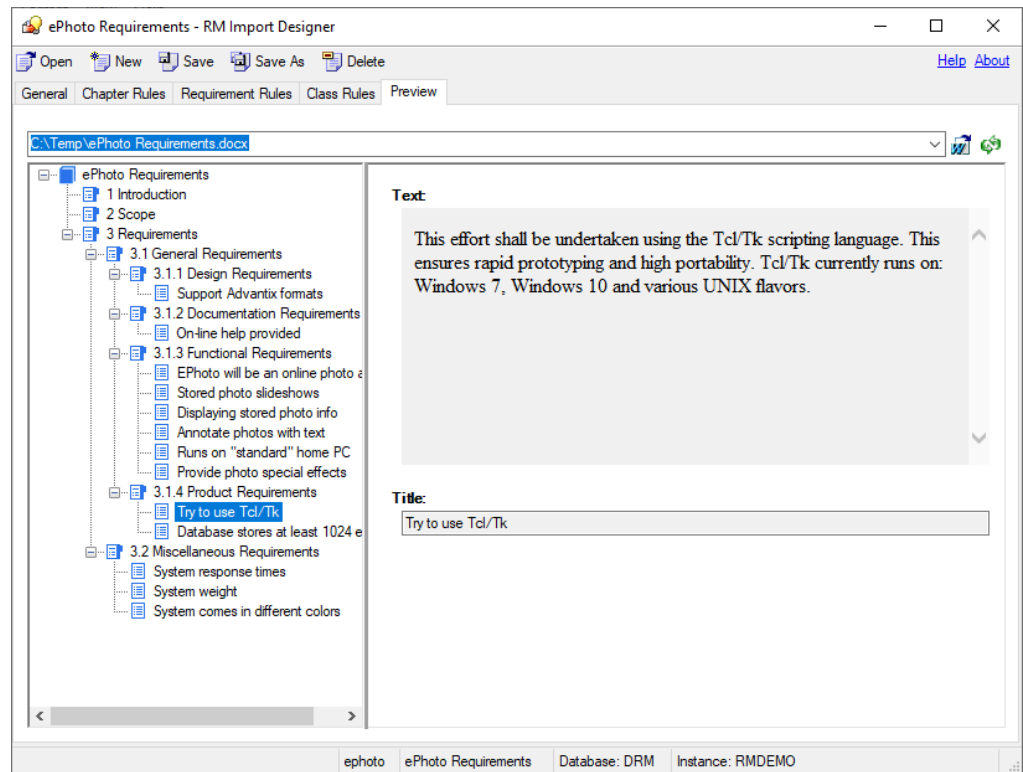
Figure 12-20. Preview Tab

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	?	**a?t** finds "act" and "art." It also finds these characters within a word (for example, "action" and "artist").
String of characters	*	**p*d** finds "pad" and "passed." The asterisk returns all characters and spaces that are between the specified literal characters.
Beginning of word	<	**<(para)** finds all words that start with "para,", such as "parakeet" and "paragraph."
End of word	>	**(out)>** finds all words that end with "out," such as "about" and "without" but not "outstanding."
One or more specified characters	[ ]	**s[io]n** 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-s]ought** 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]	**h[!a-m]ck** finds "hock," but not "hack" or "hick."
Exactly *n* occurrences of the previous character or expression	{n}	**me{2}t** finds "meet" but not "met." **h[a-z]{2}d** finds "heed," "hand," and "hind," but does not find "hid" or "had". **h([a-z]){2}d** finds "heed" but not "hand" or "hind."
At least *n* occurrences of the previous character or expression	{n,}	**lo{1,}t** finds "loot" and "lot."
From *n* to *m* occurrences of the previous character or expression	{n,m}	**30{1,3}** finds "30," "300," and "3000."
One or more occurrences of the previous character or expression	@	**ro@t** finds "rot" and "root."

Text to Search	Wildcard Character	Examples
Any wildcard character	*\wildcard_ character*	**[\?]** finds all question mark wildcards, **[*]** finds all asterisk wildcards, and so on.
To group characters and set orders of evaluation	()	**h([a-z]){2}d** 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
RQMT_[0-9]@	Finds sequences that start with "RQMT_" and any number of numbers. For example, **RQMT_0009**.
\<\<SYS[0-9]@\>\>	Finds sequences that start with <<, then "SYS" and any number of numbers, and that end with >>. for example, **<<SYS0109>>**.
[0-9].	Finds sequences that start with any number and a period. For example, **24.**.
0[0-9]@	Finds sequences that start with 0 followed by any number of numbers. For example, **0008**.
[0-9].[0-9].[0-9]	Finds sequences that start with three numbers separated by decimal points. For example, **1.2.6**.

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 491 contains examples of Word documents and explains how their structure determines how you set up templates for them.

Chapter 13
WIRIS Editor

Overview

The WIRIS editor allows to enter mathematical formulas in Dimensions RM. This functionality is only available for texts in HTML format, e.g. HTML enabled text attributes in requirements or chapters in documents. In order to use this component go to 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 *RM_Install*\Common Tools 1.8.6.0\tomcat\9.0\webapps directory.

3   Copy the `tiny_mce_wiris` directory into the *RM_Install*\Common Tools 1.8.6.0\tomcat\9.0\webapps\rtmBrowser \rm\vendor\tiny_mce\plugins directory. If the plugins directory already contains a `tiny_mce_wiris` directory, delete that directory.

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.

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*\Common Tools
1.8.6.0\tomcat\9.0\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 might look like this:
C:\\Program Files\\Micro Focus\\Dimensions 12.10\\Common Tools
1.8.6.0\\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*\Common Tools 1.8.6.0\tomcat\9.0\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.

   c   Replace the existing value (following the = sign) with `png`, so the line reads: `wirisimageformat = png`

13   To configure the editor response format:

   a   Find the variable `wirispluginperformance`.

   b   Remove the # in front of the variable.

   c   Replace the existing value (following the = sign) with `false`, so the line reads: `wirispluginperformance = false`

14   Save the file.

Configuring Dimensions RM for the WIRIS Editor

Configuring the HTML Editor

The following steps describe how to configure the WIRIS editor for the **Edit Attributes** dialog (editing HTML enabled attributes of a single requirement).

To configure the WIRIS editor for requirements and chapters, do the following:

1   Navigate to the *RM_Install*\Common Tools 1.8.6.0\tomcat\9.0\webapps\rtmBrowser\rm\common\js directory and open the file `htmlEditor.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"

  ],

  toolbar: [

   "undo redo | styleselect | bold italic forecolor backcolor fontselect fontsizeselect | 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*\Common Tools 1.8.6.0\tomcat\9.0\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: [

   "(!isNewObject ? "save cancel | " : "" ) + "bold italic forecolor
   backcolor fontselect fontsizeselect "

   + "alignleft aligncenter alignright alignjustify | bullist numlist
   outdent indent | openlink "

   + "link unlink image fullscreen qpimage mxgraph | addcaption
   addreference "

   + (rtmDdInitData.glossaryEnabled ? " | glossary" : "") + "
   tiny_mce_wiris_formulaEditor"

   + " 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*\Common Tools
    1.8.6.0\tomcat\9.0\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
fontsizeselect | alignleft aligncenter alignright alignjustify | bullist
numlist outdent indent | link unlink image fullscreen qpimage mxgraph" +
(window.suppressGlossarySupport ? "" : " | glossary | close") + "
tiny_mce_wiris_formulaEditor"

   ],
```

Restart Dimensions RM Services

After completing all settings, restart the following services:

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

Appendix A
Handling Certificates

Importing a PFX Certificate into Microsoft IIS

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

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

1   On the server, start **Server Manager**.

2   Expand **Roles**.

3   Expand **Web Server (IIS)**.

4   Select **Internet Information Services (IIS) Manager**.

5   In **Internet Information Services (IIS) Manager**, select your server.

6   On the servers **Home** view, double-click **Server Certificates**.

7   In the **Actions** pane, click **Import...**

8   Click **...**. This opens the **Open** dialog.

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

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

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

12   Click **OK**.

Importing a PFX Certificate into Windows

If you are using IIS, you only need to execute the steps described in chapter . 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 454).

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 454).

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).

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

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

1 On the server, open a command prompt.

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

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

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

5 Click **Add**.

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

   a Select **Computer account**.

   b Click **Next**.

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

   d Click **Finish**.

7 Click **OK**.

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

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

   • `Personal | Certificates`

   • `Trusted Root Certification Authorities | Certificates`

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

11 Click **Next**.

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

13 Click **Next**.

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

15 Select the following options:

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

   ● **Export all extended properties**

16 Click **Next**.

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

18 Click **Next**.

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

20 Select the target directory and specify a file name.

21 Click **Save**.

22 Click **Next**.

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

Exporting Certificates to PFX Format from IIS

A certificate in PFX format is required for import into the ssl keystore (e.g. sample-ssl.jks) in Tomcat's `conf` directory. For all other keystores, use the CER format (see chapter).

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

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

1 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 458).

To export the STS certificate, do the following:

1 From a command prompt, navigate to the following directory on the STS server:
`TokenService.war\WEB-INF\conf`

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

> **NOTE**
>
> - Replace *RM_Install* with the path to the Dimensions RM directory, e.g. *C:\Program Files\Micro Focus\Dimensions 12.10*.
>
> - Replace *#.#.#.#* with the Common Tools version number, e.g. *1.8.6.0*.
>
> - Replace *#.#* with the Java version number, e.g. 11.0.
>
> The complete set command may look like this:
>
> `set path=%path%;"`*`C:\Program Files\Micro Focus\Dimensions`*` 12.10\Common Tools `*`1.8.6.0`*`\jre\`*`11.0`*`\bin"`

3 Type the following command (all on one line) and press **Enter**:
`keytool -export`
`-keystore keystore.jks -storepass `*`StorePassword`*
`-alias sts -file `*`CerPath`*

> **NOTE**
>
> - Replace *StorePassword* with the password for the keystore. The default for keystore.jks is **changeit**
>
> - Replace *CerPath* with the full path to your certificate in CER format. If the path contains spaces, surround the path with double quotes.
>
> The complete keytool command may look like this (all on one line):
>
> `keytool -export -keystore keystore.jks -storepass `*`MyPassword`*
> `-alias sts -file `*`"C:\My Certificates\MyCert.cer"`*

4   To convert the certificate to PEM format, type the following openssl command and press **Enter**:

```
openssl x509 -in CerPath -inform DER -out PemPath -outform PEM
```

> **NOTE**
>
> - You can obtain an openssl binary from http://www.openssl.org/.
>
> - Replace *CerPath* with the full path to your certificate in CER format. If the path contains spaces, surround the path with double quotes.
>
> - Replace *PemPath* with the full path you want to save the certificate in PEM format to. If the path contains spaces, surround the path with double quotes.
>
> The complete keytool command may look like this (all on one line):
>
> ```
> openssl x509 -in "C:\My Certificates\MyCert.cer" -inform DER
> -out "C:\My Certificates\MyCert.pem" -outform PEM
> ```

Exporting the STS Certificate from SBM Configurator

When using SBM, you can export the STS certificate through SBM configurator, which allows exporting the certificate into various formats.

To export the STS certificate, do the following:

1   Start **SBM Configurator**.

2   In the **Advanced** set, select **Security**.

3   In the **Components** list, ensure that **STS** is selected.

4   Click **Actions**. This opens a shortcut menu.

5   From the shortcut menu, select **Export Certificate**. This opens the **Save As** dialog.

6   In the **Save as type** box, select the desired format.

> **NOTE**
>
> - If you require the certificate for copying it to *RM_Install*\RM\conf, choose **(*.pem)**.
>
> - If you require the certificate for importing it into a keystore (e.g. truststore.jks), choose **(*.cer)**.

7   Navigate to a directory to which you want to save the file to.

8   Enter a file name (e.g. `sts.pem` or **sts.cer** depending on the Save as type setting) into the **File name** box.

9   Click **Save** and confirm the success message.

Listing all Certificates in a Keystore

To retrieve the alias, execute these steps:

1 Open a command prompt and navigate to the directory where the keystore is located.

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

> **NOTE**
>
> ■ Replace *RM_Install* with the path to the Dimensions RM directory, e.g. *C:\Program Files\Micro Focus\Dimensions 12.10*.
>
> ■ Replace *#.#.#.#* with the Common Tools version number, e.g. *1.8.6.0*.
>
> ■ Replace *#.#* with the Java version number, e.g. 11.0.
>
> The complete set command may look like this:
>
> `set path=%path%;"`*`C:\Program Files\Micro Focus\Dimensions`*` 12.10\Comm on Tools `*`1.8.6.0`*`\jre\`*`11.0`*`\bin"`

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

> **NOTE**
>
> ■ Replace *Keystore* with the path to the desired keystore. If the path contains spaces, surround the path with double quotes.
>
> ■ Replace *StorePassword* with the password for the keystore.
>
> The complete keytool command may look like this (all on one line):
>
> `keytool -list -v -keystore `*`sample-ssl.jks`*` -storepass `*`serena`*`
> >certs.txt`

4 Type `notepad certs.txt` and press **Enter**. This opens the file certs.txt in Notepad. The file certs.txt contains detailed information about all certificates in the keystore.

Retrieving the Alias from a PFX File

When importing the certificate into the Micro Focus Common Tomcat, the alias used in the PFX file is required.

To retrieve the alias, execute these steps:

1 Open a command prompt and navigate to the directory where the PFX file is located.

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

> **NOTE**
>
> ■ Replace *RM_Install* with the path to the Dimensions RM directory, e.g. *C:\Program Files\Micro Focus\Dimensions 12.10*.
>
> ■ Replace **#.#.#.#** with the Common Tools version number, e.g. *1.8.6.0*.
>
> ■ Replace **#.#** with the Java version number, e.g. *11.0*.
>
> The complete set command may look like this:
>
> `set path=%path%;"`*`C:\Program Files\Micro Focus\Dimensions`*` 12.10\Comm on Tools `*`1.8.6.0`*`\jre\`*`11.0`*`\bin"`

3 Type the following command (all on one line) and press **Enter**:
`keytool -list -v`
`-keystore `*`PfxCertificate`*` -storepass `*`PfxPassword`*` >pfx.txt`

> **NOTE**
>
> ■ Replace *PfxCertificate* with the file name of your PFX certificate. If the file name contains spaces, surround the file name with double quotes.
>
> ■ Replace *PfxPassword* with the password for the PFX certificate. If you exported the certificate as described in chapter "Exporting Certificates to PFX Format from the Management Console," use the password you specified on export.
>
> The complete keytool command may look like this (all on one line):
>
> `keytool -list -v`
> `-keystore `*`MyCertificate.pfx`*` -storepass `*`topsecret`*` >certs.txt`

4 Type `notepad pfx.txt` and press **Enter**. This opens the file pfx.txt in Notepad.

5 Locate the line starting with **Alias name** and write down the value. In this example, the alias name is 1: `Alias name:` *1*

Retrieving Root CA and Intermediate CA Certificate Files from a Certificate

A certificate usually contains several Certification Authority certificates, which confirm the validity. If you require the certificates of these certificates as separate files, you need to extract them from the certificate. The following steps show how to that for both, PFX and CER certificates.

A certificate path may look like this:

■ `Root CA`

    ■ `Intermediate CA`

        • `Server`

There may be several intermediate CAs in a certificate. If you require the intermediate CA files, you need to export all of them.

Retrieving Root CA and Intermediate CA Certificate Files from a PFX File

As PFX files cannot be opened directly, you need to open it in the Certificate Manager.

To open a PFX certificate in the Certificate Manager, execute these steps:

1 Open a command prompt.

2 Type `certmgr` and press **Enter**. This starts the Certificate Manager.

3 Locate the certificate in the tree. A common location may be `Personal | Certificates`.

If you cannot find the certificate, you need to (temporarily) import it by executing these steps:

a Right-click the **Personal** folder. In the shortcut menu, point to **All Tasks**, and then select **Import...**. This opens the **Certificate Import Wizard**.

b Click **Next**.

c Click **Browse...**.

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

e Select the PFX file and click **Open**.

f Click **Next**.

g In the **Password** box, type the current password for the PFX file.

h Click **Next**.

i Click **Next**.

j Click **Finish** to import the file and confirm the success message.

k In the tree, expand **Personal**, then select **Certificates**.

4 Double-click the Certificate. This opens the **Certificate** dialog. Continue with step 2 in chapter .

Retrieving Root CA and Intermediate CA Certificate Files from a CER File

The following steps describe how to retrieve root CA and intermediate CA certificates from a server certificate file in CER format. Depending on your certificate, there may be no root CA and/or intermediate CA certificates.

To retrieve root CA and intermediate CA certificate files from a CER file, do the following:

1 Double-click the CER file. This opens the **Certificate** dialog.

2 Select the **Certification Path** tab.

3 If you see only one entry (your server name), there are no root CA and intermediate CAs. Skip all further steps.

4 Select the top certificate (this is the root CA).

5 Click **View Certificate**. This opens the selected certificate.

6 Select the **Details** tab.

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

8 Click **Next**.

9 Select the export format, e.g. **DER-encoded binary X.509 (.CER)**.

10 Click **Next**.

11 Click **Browse...** to specify the path/file name to which you want to export the certificate.

12 Click **Next**.

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

14 Click **OK** to close the certificate.

15 If there are certificates between the root CA certificate and the server certificate, select each of them and execute steps 5-14.

Importing Root CA and Intermediate CA certificates into the Local Machine Certificate Store

To import a root CA certificate and/or an intermediate CA certificate in CER format, do the following:

1 On the server, open a command prompt.

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

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

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

5 Click **Add**.

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

  a Select **Computer account**.

  b Click **Next**.

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

  d Click **Finish**.

7 Click **OK**.

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

9 To import a **root CA certificate**, do the following:

   a Right-click **Trusted Root Certification Authorities**. This opens a shortcut menu.

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

   c Click **Next**.

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

   e In the file filter box, select **X.509 Certificate (*.cer;*.crt)**.

   f Select the CER certificate and click **Open**.

   g Click **Next**.

   h Click **Next**.

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

10 To import an **intermediate CA certificate**, do the following:

   a Right-click **Intermediate Certification Authorities**. This opens a shortcut menu.

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

   c Click **Next**.

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

   e In the file filter box, select **X.509 Certificate (*.cer;*.crt)**.

   f Select the CER certificate and click **Open**.

   g Click **Next**.

   h Click **Next**.

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

Appendix B

Database Security

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 "Native Network Encryption with Oracle" on page 471)

++ 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 "Transport Encryption with Oracle" on page 466)

+ 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 one 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:

- Micro Focus SyncEngine and any other SyncEngine service

- Micro Focus Common Tomcat

- Micro Focus Dimensions RM Pool Manager

- Micro Focus ALF Event Emitter

- Micro Focus 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 Micro Focus Common Tomcat, users of those applications will also be unable to work.

3 Execute the steps described in chapter "Database Server Configuration" on page 467.

4 Execute the steps described in chapter "Dimensions RM Application Server and Admin Client Configuration" on page 469.

5 Start the services you shut down in step 2 in this order:

- Micro Focus Dimensions RM Pool Manager

- Micro Focus Common Tomcat

- Micro Focus ALF Event Emitter

- Micro Focus Dimensions RM E-Mail Notification Service

- Micro Focus 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 469.

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 466).

> **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_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 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
-dn "CN=dbcert" -keysize 1024 -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 from a Certificate" on page 460.

> **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 *1777* with the port number you wish to use with your environment.

12 Save the file.

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 466).

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.

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:

   • Micro Focus SyncEngine and any other SyncEngine services

   • Micro Focus Common Tomcat

   • Micro Focus Dimensions RM Pool Manager

- Micro Focus ALF Event Emitter

- Micro Focus 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 185. 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 480.

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:

- Micro Focus Dimensions RM Pool Manager

- Micro Focus Common Tomcat

- Micro Focus ALF Event Emitter (if it was running before)

- Micro Focus Dimensions RM E-Mail Notification Service (if it was running before)

- Micro Focus 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 476). 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 477

- **SQL Server 2016/2017:** see chapter "Installing a Certificate for SQL Server 2019" on page 479

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 CA and Intermediate CA certificates into the Local Machine Certificate Store" on page 462.

  If you do not have the root CA/intermediate CA certificate files, see chapter "Retrieving Root CA and Intermediate CA Certificate Files from a Certificate" on page 460 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 from a Certificate" on page 460 and "Importing Root CA and Intermediate CA certificates into the Local Machine Certificate Store" on page 462).

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 from a Certificate" on page 460 and "Importing Root CA and Intermediate CA certificates into the Local Machine Certificate Store" on page 462).

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:

   • Micro Focus SyncEngine and any other SyncEngine services

   • Micro Focus Common Tomcat

   • Micro Focus Dimensions RM Pool Manager

- Micro Focus ALF Event Emitter

- Micro Focus 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 185. 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 480.

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:

   • Micro Focus Dimensions RM Pool Manager

   • Micro Focus Common Tomcat

   • Micro Focus ALF Event Emitter (if it was running before)

   • Micro Focus Dimensions RM E-Mail Notification Service (if it was running before)

   • Micro Focus 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

The database encryption feature is a security measure designed to address the fact that there was a static, hard-coded password for the ICADMIN and ICPROJECT Oracle accounts. 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 233.

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 **Change User** from the context menu. If you get the same error message again instead of a prompt to log in, then there is probably no instance in the database instance.
2	You know a Dimensions RM instance exists. The security file could be in the wrong location.	In RM Manage, select **Workspace	Options**. Click the **Security** tab and verify the location and name of the security file.
3	You know the security file is in the correct location. 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 **Convert Database**. When the database validation tool starts, select your instance and click **Upgrade**. When it prompts whether you want to recreate the stored procedures, click **Yes**.

4	The ICADMIN account could be locked.	In SQL Plus, try to log in as ICADMIN by typing the following command:
		
		`sqlplus icadmin/<dummy`
		`    password>@<database instance>`
		
		If Oracle returns a message that the account is locked, type the following commands to unlock it:
		
		`sqlplus icdba/icdba@<database instance>`
		`alter user icadmin account unlock;`
		`exit`

5	The Dimensions RM or Oracle path could be wrong.	In RM Manage, select **Workspace	Options**. Click the **Mandatory** tab, and confirm that the **RTM_HOME** and **ORACLE_HOME** values are correct.

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*.

Exporting Documents creates DOC Files

Document export creates DOC files under these conditions:

- Microsoft Word is not installed on the server or the installed version is not supported.

- The server is not prepared for export. For information on how to prepare your server, refer to *"Support for Export/Import"* in the *Dimensions RM Installation Guide*.

- If Word fails on opening a DOC file, refer to .

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 517.

Improving Poor Performance

Please consult Oracle documentation or your database administrator (DBA) for tuning changes that could improve performance. For example, you might change the CURSOR_SHARING parameter to "force" or change the STATISTICS_LEVEL parameter to "all."

Empty Window in Internet Explorer 11

When using Internet Explorer 11 with Windows's built-in Administrator account, there might be situations when an empty window remains on the screen. If you need to use the built-in Administrator account, follow these steps to change the Admin approval mode and solve the problem:

1   Open a command prompt.

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

3   Open the **Local Policies** folder.

4   Select the **Security Options** folder.

5   Locate the item **User Account Control: Admin Approval Mode for the Built-in Administrator account** and double-click it.

6   Set the value to **Enabled**.

7   Click the **OK** button.

8   Restart the computer.

Disabling the Compatibility View in Internet Explorer

Using Internet Explorer's Compatibility View is not recommended with RM Browser. To turn off Compatibility View, follow these steps:

1   Open Internet Explorer.

2   Click the cog in the top right corner to open the menu.

3   In menu, select **Compatibility View Settings** to open the related dialog.

4   Clear the **Display intranet Sites in Compatibility View** box.

5   If the server is listed in the list of websites, do the following:

    a   Select the server in the list.

    b   Click **Remove**.

6   Click **Close** to close the **Compatibility View Settings** dialog.

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.

Poor Performance with MS SQL Server

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**.

Appendix D

RM Import Designer Examples

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.
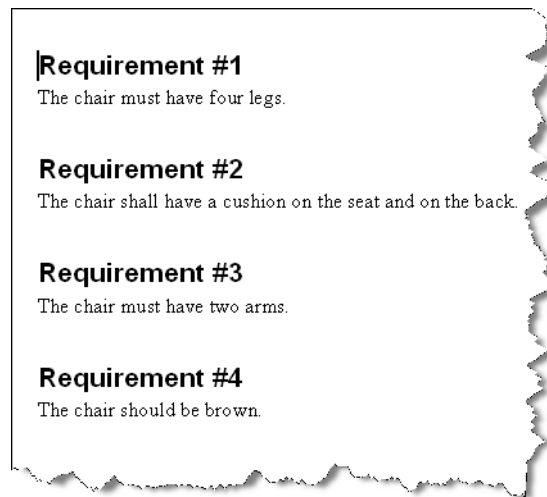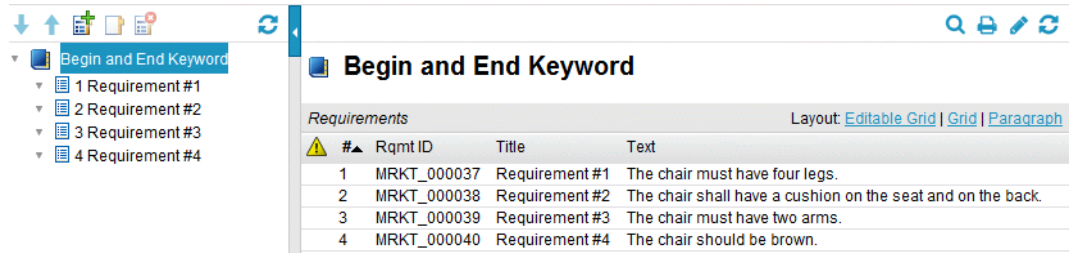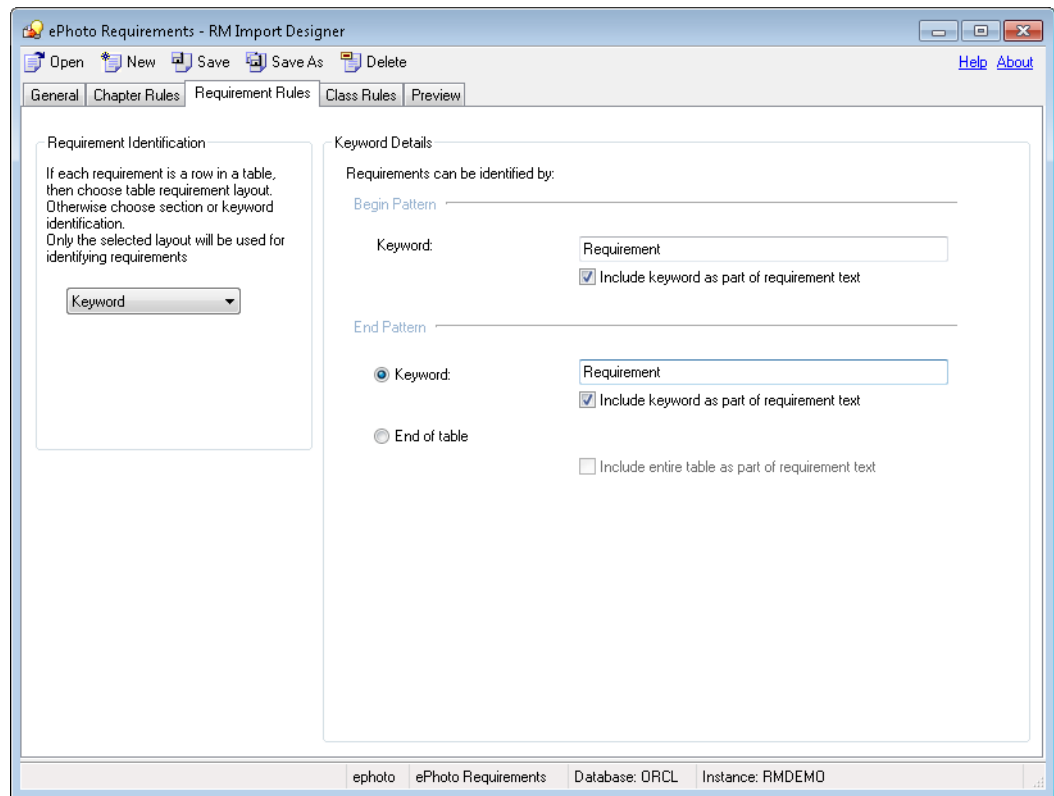
Entire Table with a Keyword is the Requirement

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.

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

3.1 General Requirements

3.1.1 Design Requirements

#	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.

3.1.2 Documentation Requirements

#	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.

3.1.3 Functional Requirements

#	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.
	KT_000001	Stored photo	The ePhoto system shall provide the ability creat
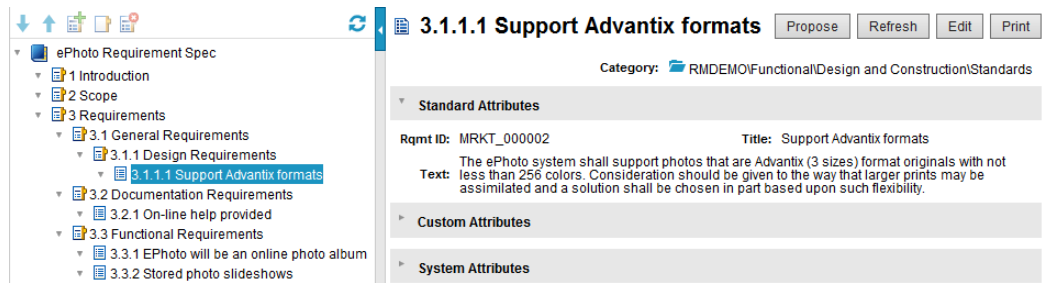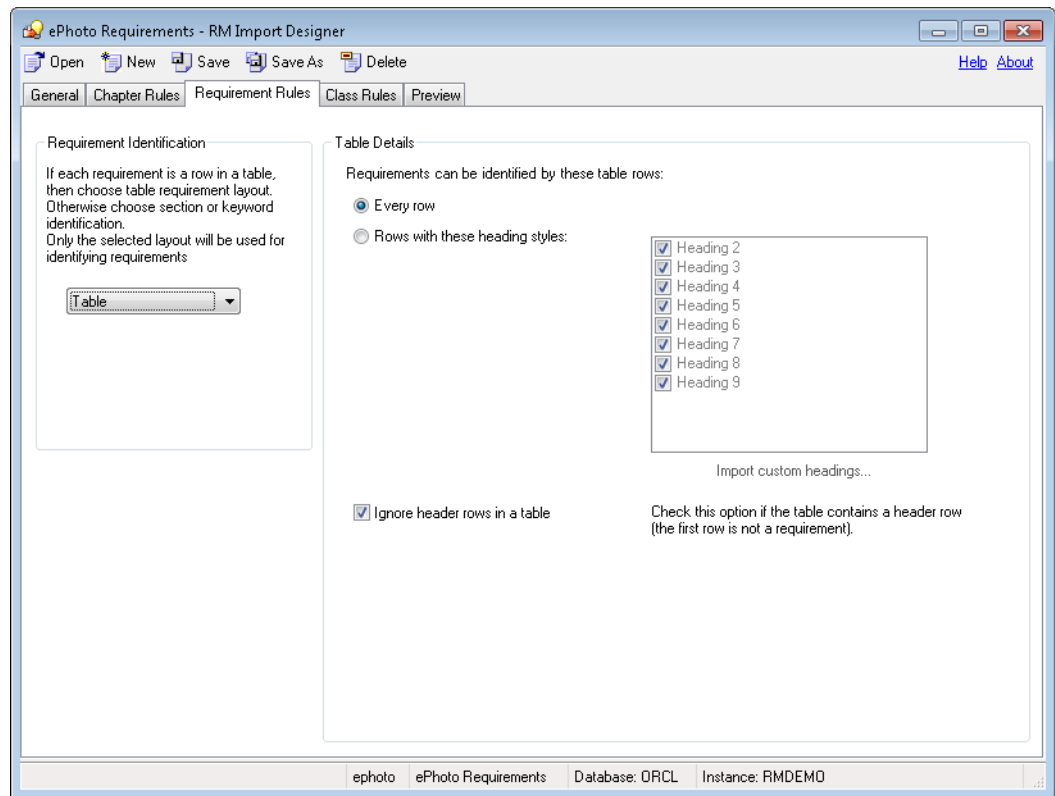
Section Option with Keywords

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.
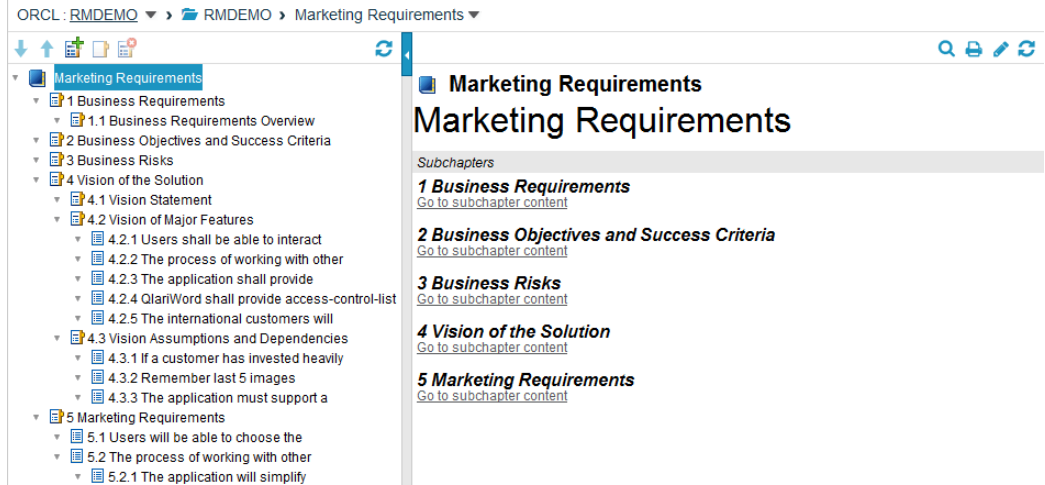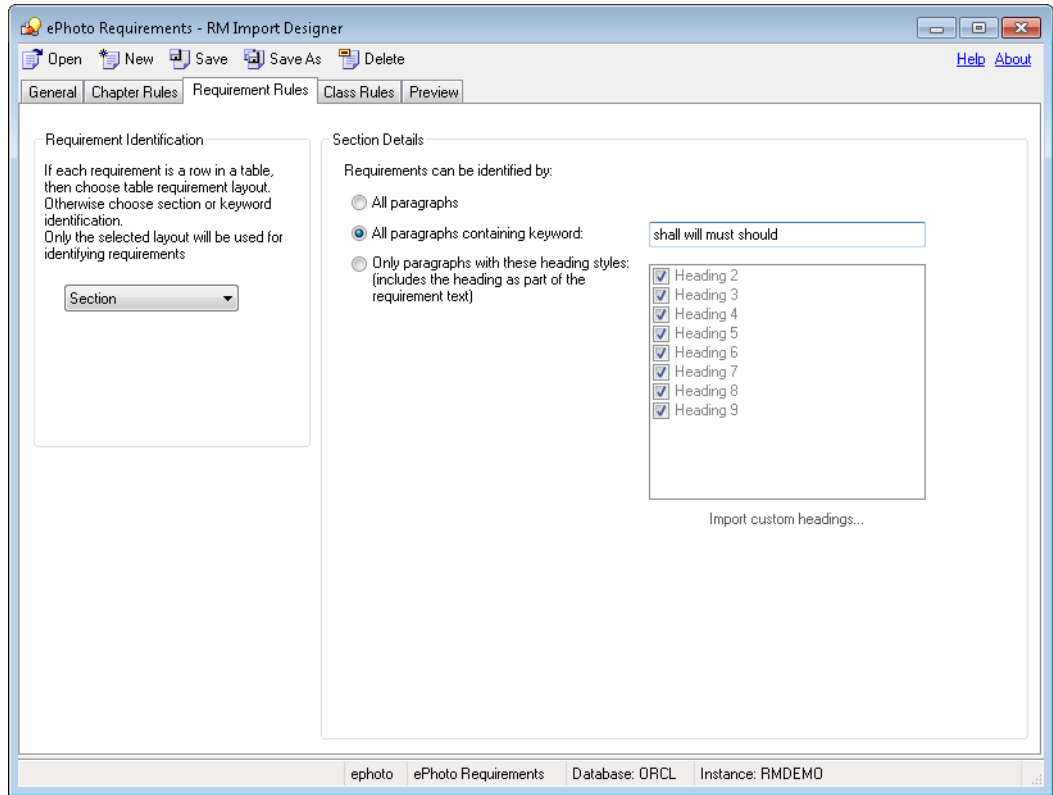
Heading Styles

In this example, the Section layout is used. Color, Make, Model, and Age have the Heading 2 style, while Car is a Heading 1 and therefore is not captured as a requirement.
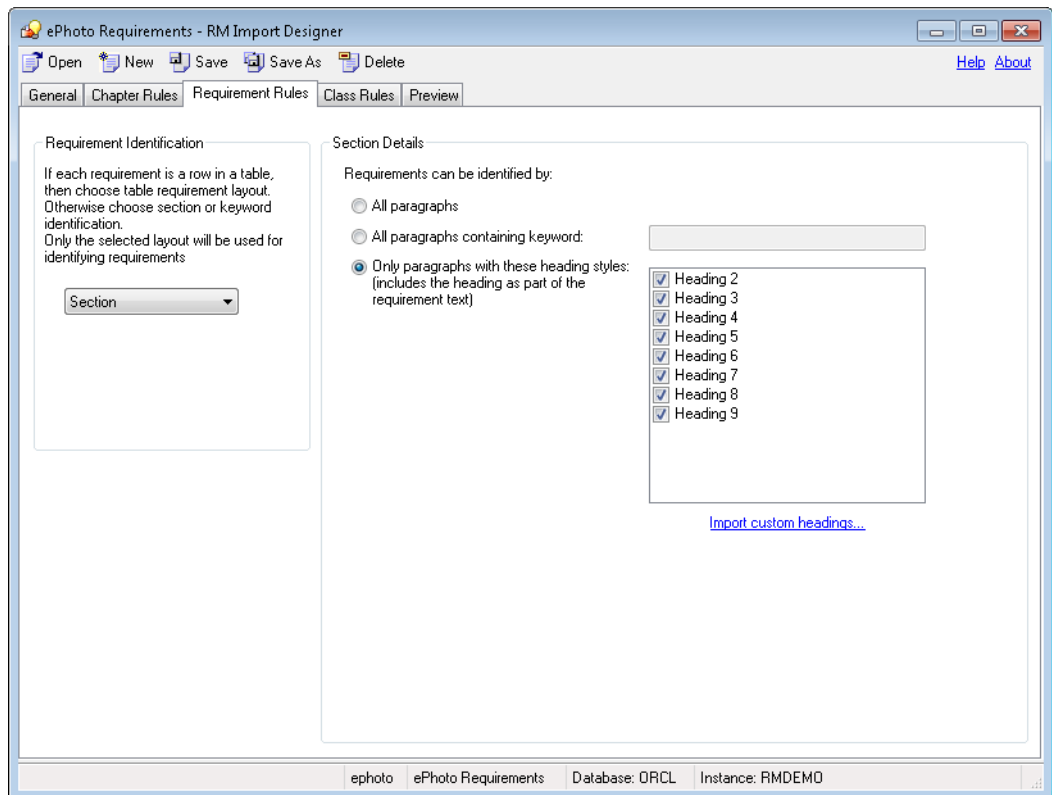
Capturing Title and Description with No Title Rule

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 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.
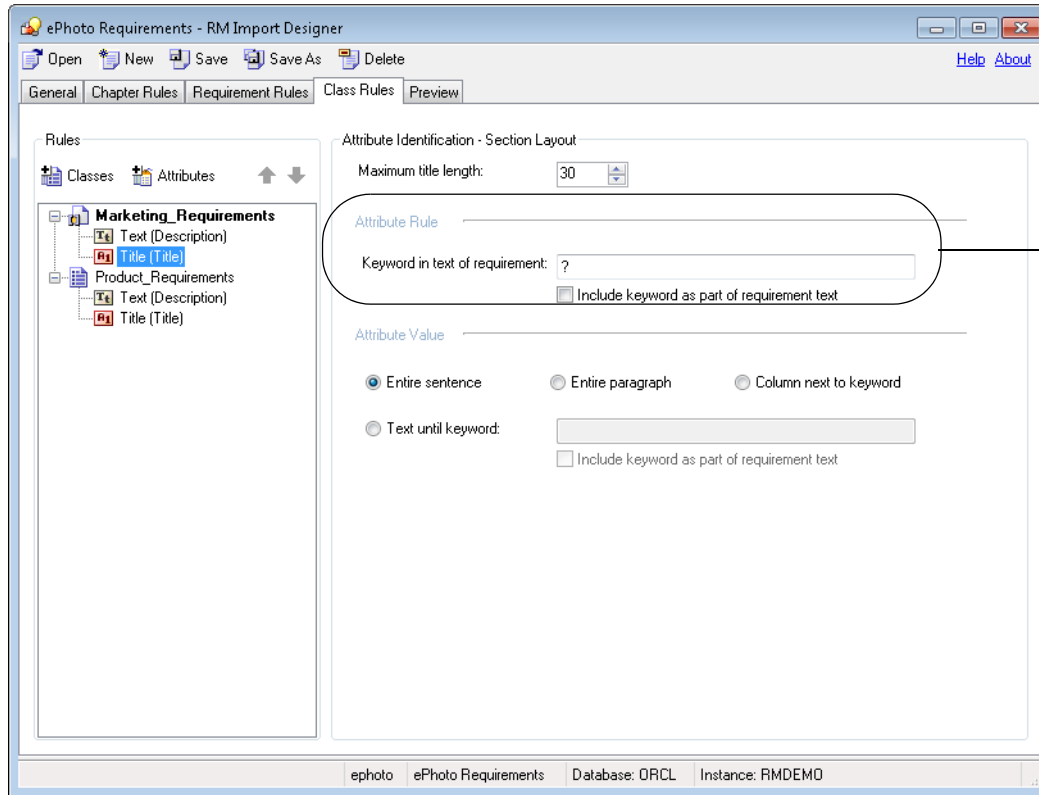
A rule is specified, so there is no duplication between the **Text** and **Title** fields below.
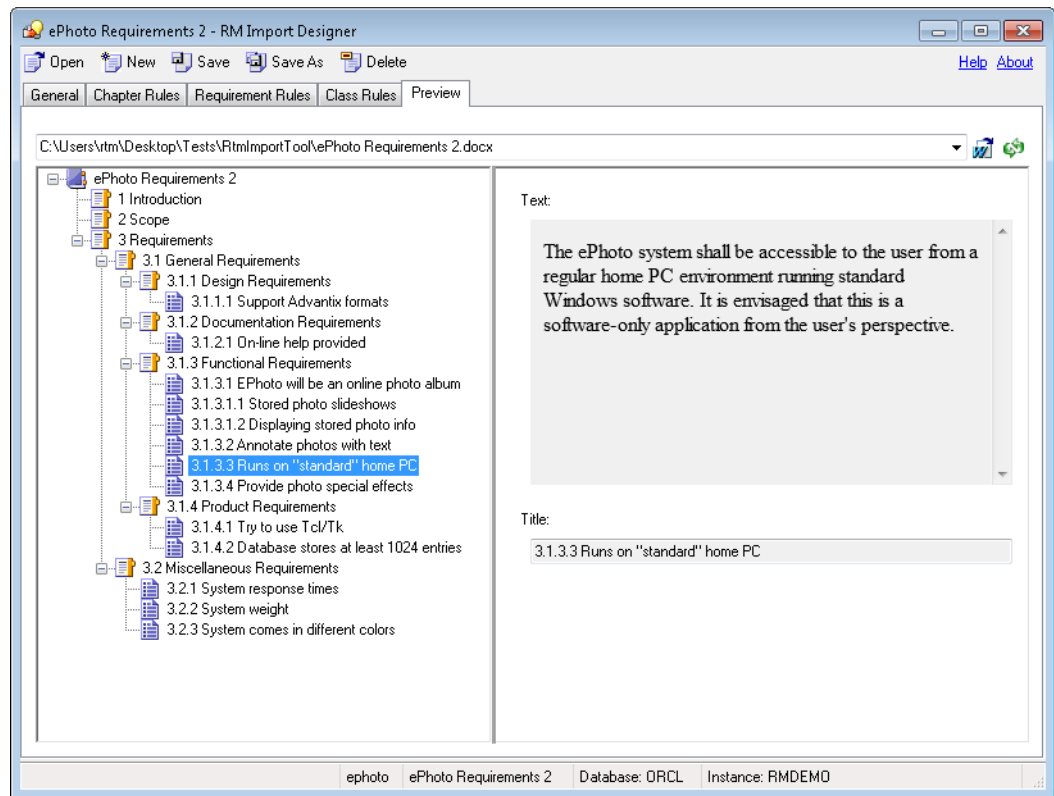
NOTE For more information about wildcards, see "Word Regular Expressions" on page 437 and Microsoft Word documentation.

Appendix E
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/
    ?goto=doc&db=DataBaseName&proj=InstanceName&doc=DocumentName
```

URL to a Chapter of a Document

```
http://ServerName/rtmBrowser/
    ?goto=doc&db=DataBaseName&proj=InstanceName&doc=DocumentName&class=
    Chapter&o=ChapterID
```

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=Colle
    ctionName
```

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 **&editableGrid=true** to the URL.	`http:// myserver:8080/ rtmBrowser/cgi-bin/ rtmBrowser.exe?goto =collection&db=ORCL &proj=RMDEMO&collec tion=CollectionName` **&editableGrid=true**
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 **&hideTitleBar=true** to the URL.	`http:// myserver:8080/ rtmBrowser/cgi-bin/ rtmBrowser.exe?goto =collection&db=ORCL &proj=RMDEMO&collec tion=CollectionName` **&hideTitleBar=true**

URL to a Specific Version of a Requirement

```
http://ServerName/rtmBrowser/
    ?goto=req&db=DataBaseName&proj=InstanceName&class=ClassName&puid=Re
    quiement'sPUID&ver=VersionNumber
```

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=Objec
    tID1&comparewithID=ObjectID2
```

Compare Current Requirement with Object Id

```
http://ServerName/rtmBrowser/
    ?goto=req&db=DataBaseName&proj=InstanceName&class=ClassName&puid=Re
    quiement'sPUID&comparewithID=ObjectID
```

Compare Requirement by Object Id and Version

```
hhttp://ServerName/rtmBrowser/
    ?goto=req&db=DataBaseName&proj=InstanceName&class=ClassName&o=Objec
    tID&comparewith=Version
```

Compare Two Versions of a Requirement

```
http://ServerName/rtmBrowser/
    ?goto=req&db=DataBaseName&proj=InstanceName&class=ClassName&puid=Re
    quiement'sPUID&ver=Version1&comparewith=Version2
```

Compare Current Requirement with a Version

```
http://ServerName/rtmBrowser/
    ?goto=req&db=DataBaseName&proj=InstanceName&class=ClassName&puid=Re
    quiement'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=ephoto
pwd=	RM password	pwd=rtm

URL to the Current Version of a Requirement

```
http://ServerName/rtmBrowser/
    ?d=DataBaseName&p=InstanceName&f=2&c=ClassID&id=Requiement'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. ■ f=2: Opens an object for viewing. ■ f=4: Opens an edit dialog for the specified object. ■ f=5: Opens the RM browser home page.	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=ephoto
pwd=	RM password	pwd=rtm

Appendix F

Running Scripts from the Command Line

Overview

Dimensions RM provides doc_out as the command line tool. doc_out allows you to run scripts from the DOS prompt. The command line tool can be run when you want to create large reports on links among entities created in or removed from the database.

Setting Your Path

The **doc_out** tool is normally installed in *RTM_HOME\bin*. The default for *RTM_HOME* is: *C:\Program Files\Micro Focus\Dimensions 12.10\RM*. The path may be different on your machine. This "bin" directory must be in your path for the doc_out tool if you want to use it in the command line without specifying the full path. If you do not know the path of your Dimensions RM installation, you can search for the tool (`doc_out.exe`) using the **Search** command from the Windows **Start** menu.

To add the Dimensions RM bin directory to your path:

1   Right-click the **My Computer** icon on your desktop.

2   Select **Properties**.

3   Click the **Environment** tab.

4   Select the **Path** variable from the system variables list.

5   In the **Value** box at the bottom of the page, insert the Dimensions RM bin path into the value string. Separate that path from the next one with a semi-colon (;).

6   Click **Set**, **Apply**, and then **OK**.

Using doc_out

The doc_out tool allows you to run a Dimensions RM reporting script from the command line and to generate the output to a variety of formats. Using doc_out enables you to extract data from Dimensions RM without invoking a Windows-based Dimensions RM session. Scripts can be prepared before extraction for batch processing of reports.

Invoking doc_out

To invoke the doc_out tool:

Type the following command at the command line prompt:

```
doc_out   required_arguments   [optional_arguments]
script_identification
```

where:

`required_arguments` are:

```
-user username -pwd password -project instancename -location dblocation
```

- **username** is your Dimensions RM user account name.

- **password** is your Dimensions RM user account password.

- **instancename** is the instance from which you want to extract data.

- **dblocation** is the database name in which the instance resides.

  - **Oracle:** Your local *tnsnames.ora* file contains the database names of each database to which you have visibility.

  - **SQL Server:** The connection name specified in the **System DSN** settings of **ODBC Data Source Administrator (64-bit)**, which is located under `C:\Windows\system32\odbcad32.exe`.

  - **PostgreSQL:** The connection name specified in the **System DSN** settings of **ODBC Data Source Administrator (64-bit)**, which is located under `C:\Windows\system32\odbcad32.exe`.

optional_arguments are:

```
[-m format] [-#variablename value]* [-o outputfile] [-e] [-v] [-s[n|u
terminatorstring]
```

- **format**–The format in which you want the output to be represented. The accepted formats are described in the following table.

Format	Description
csv	Comma Separated Values format
rtf	Rich text format used by Microsoft Word
rtf_table	Rich text table format
sgml	SGML markup format
sgml_table	SGML table format
html	HTML format
html_table	HTML table format
none	No markup (that is, plain ASCII)
ascii_table	ASCII text with spacing to create a tabular effect. **NOTE:** This is the default output format.

- **variablename** is the name of a variable defined in the script and **value** is the actual value that you want substituted for that variable. You will need to define **- #variablename value** pairs for each variable defined in the script.

- **outputfile** is the filename or path in which the results are to be stored. Enclose the path in double quotation marks when spaces or punctuation characters are included in the filename.

- **-e** suppresses word processor markup at the beginning of the outputfile (not accepted for RTF or SGML formats). Omitting markup is useful when you will be appending the output to an existing file.

- **-v** requests program arguments be echoed to the console or DOS window.

- **-s** (used only with the -m none option) with no argument causes a standard end-of-record marker ("#### End of Record ####") to be appended to each record in the report.

- -su (used only with the -m none option) terminatorstring provides a textual end-of-record marker for the -su option. Enclose terminatorstring in double quotation marks when spaces or punctuation characters are included the string.

- -sn (used only with the -m none option) eliminates blank lines in the unformatted output. Blank lines are otherwise inserted for empty attribute values. -sn can be used in combination with -su, but overrides -s.

script_identification is:

scriptfilename | -n scriptname

- scriptfilename is the path of the script stored in the file system.

- -n scriptname identifies a script stored in the instance. Scriptname is required with the -n option. If the script name in the instance includes blanks or punctuation characters, you will need to enclose the name in double quotes (for example, -n "my favorite script").

Using doc_out from the Command Line

Various ways to use the doc_out tool from the command line are illustrated in the following DOS examples.

Example 1

Minimum arguments. Assumes that doc_out is in the path, the script text is in the current folder, and the results are to be displayed on the screen. The output format defaults to ascii_table.

```
C:\>doc_out -user fred -pwd fredspassword
-project myinstance -location bigserver.ic
getCustomerRequirements.rmdoc
```

Example 2

Similar to Example 1, but references a script inside the instance and an output file in the current folder in which to save the results.

```
C:\>doc_out -user fred -pwd fredspassword
-project myinstance -location bigserver.ic
-n "Get Customer Requirements" -o CustomerRequirements.txt
```

Example 3

Similar to Example 2, but requests the output in a csv file that can then be imported into other tools.

```
C:\>doc_out -user fred -pwd fredspassword -project
myinstance -location bigserver.ic -n "Get Customer
Requirements" -m CSV
-o CustomerRequirements.csv
```

Example 4

Similar to example 2, but specifies no markup and uses the date as a record separator.

```
C:\>doc_out -user fred -pwd fredspassword -project
myinstance -location bigserver.ic -n "Get Customer
```

```
Requirements” -m none -su “09/15/2000”
-o CustomerRequirements.txt
```

Example 5

Similar to Example 3, but uses a variable to specify a collection that identifies a subset of the objects

```
C:\>doc_out -user fred -pwd fredspassword -project myinstance
-location bigserver.ic -#LookIn Baseline1 -n “Get
Customer Requirements” -m CSV -o CustomerRequirements.csv
```

Using Script Variables with doc_out

Variables can be used within a Dimensions RM reporting scripts only when the script is run by doc_out. Attempting to use them in RM Browser results in erroneous results because the variable values are substituted in doc_out before submitting the script to Dimensions RM.

To use variables in scripts, follow these rules:

- Use UPPER CASE for the variable name in both the script and the command line reference.

- Enclose spaces or punctuation in values in double quotation marks.

- In the command line, precede the variable name with a '#', but in the script, include the variable name without any special markings.

The following example is a parameterized version of the baseline check script provided in the RMDEMO sample instance. The script identifies three subsets of objects given two collections used as baselines. The first subset is (the first select statement) the set of objects in the earlier baseline that are not deleted and are still in the later baseline (as identified by the second select statement). The second subset is those objects that are in the later baseline, but were not in the earlier baseline. The third subset is those objects that were in the earlier baseline and were deleted.

```
select  <PUID>PUID <Earlier>TEXT from CustomerRequirements where
group in ('EARLY') and STATUS != 'Deleted'
xref source secondary_history
select  <PUID>PUID <Later Modifications>TEXT from
CustomerRequirements where group in ('LATE')
plus
select  <PUID>PUID <Later Additions>TEXT from CustomerRequirements
where group in ('LATE')  and group not in  ('EARLY')  and
NOT_SECONDARY_IN immediate
plus
select  <PUID>PUID <Earlier Deletions>TEXT from
CustomerRequirements where group in ('EARLY') and STATUS='Deleted'
```

The baseline check script is invoked to compare Baseline 1 and Baseline 2 from the DOS command line as:

```
C:\>doc_out -user fred -pwd fredspassword -project rmdemo
-location bigserver.ic baselinecheck.rmdoc -#EARLY
“Baseline 1” -#LATE “Baseline 2”
```

Appendix G
Word Document 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 .

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	If enabled, Word Document Post Processor converts HTML lists to Word lists. **Possible values:** ■ False ■ True **Default: True** (turned on).
List_Styles	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.
List_Style_L1...9	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. **Default (for level 1): margin-left:72.0pt;mso-add-space:auto;text-indent:-18.0pt;**
RemoveStyles	If enabled, Word Document Post Processor removes <style> tags within the body of the document. **Possible values:** ■ False ■ True **Default: True** (turned on).
RemoveUnreferencedLists	If enabled, Word Document Post Processor removes styles for lists which are not present in the document. **Possible values:** ■ False ■ True **Default: True** (turned on).

Setting	Description
WordBulletListStyle_L1...9	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. **Possible values:** - Bullet_Simple - Bullet_Empty - Bullet_Square - Bullet_Color - Bullet_Diamond - Bullet_Arrow - Bullet_Tick **Defaults:** **WordBulletListStyle_L1: Bullet_Simple** **WordBulletListStyle_L2: Bullet_Empty** **WordBulletListStyle_L3...9: Bullet_Square**
WordNumericListStyle_L1...9	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. **Possible values:** - Number_Simple - Number_Parenthesis_Closing - Number_Parenthesis_Surrounding - Number_Abc_Lowercase - Number_Abc_Lowercase_Parenthesis_Closing - Number_Abc_Uppercase - Number_Abc_Uppercase_Parenthesis_Closing - Number_Roman_Capital - Number_Roman_Lowercase - Number_Greek_Lowercase **Defaults:** **WordNumericListStyle_L1: Number_Simple** **WordNumericListStyle_L2: Number_Abc_Lowercase** **WordNumericListStyle_L3...9: Number_Simple**

Image Settings

Setting	Description
CorrectImageSize	If enabled, Word Document Post Processor resizes images to fit the page. **Possible values:** ■ False ■ True **Default: True** (turned on).
ImgSubstractWidthInPixels	Defines the number of pixels which to subtract from an image when resizing it. **Possible values:** ■ Any integer (whole number) which is 0 or larger. **Default: 10**.
MarginLeft	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. **Default: 1.25 in**
MarginRight	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. **Default: 1.25 in**
PageHeight	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. **Default: 841.9 pt**
PageWidth	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. **Default: 595.3 pt**

Other Settings

Setting	Description
CorrectEmptyParagraphs	If enabled, Word Document Post Processor corrects empty paragraphs. **Possible values:** ■ False ■ True **Default: True** (turned on).
IntegrateSubdocuments	If enabled, Word Document Post Processor integrates sub-documents into the main document and converts the the encoding. **Possible values:** ■ False ■ True **Default: True** (turned on).
RemoveStyles	If enabled, Word Document Post Processor removes <style> tags within the body of the document. **Possible values:** ■ False ■ True **Default: True** (turned on).
RemoveTableSize	If enabled, Word Document Post Processor removes the width setting for tables. **Possible values:** ■ False ■ True **Default: True** (turned on).
RemoveUnwantedTags	If enabled, Word Document Post Processor removes HTML undesired HTML tags. **Possible values:** ■ False ■ True **Default: True** (turned on).

Setting	Description
RemoveVfTags	If enabled, Word Document Post Processor removes V:F tags and any parent tags in the "V" namespace. **Possible values:** ■ False ■ True **Default: True** (turned on).
RemoveWordSection1	If enabled, Word Document Post Processor removes excess WordSection1 or Section1 class names. **Possible values:** ■ False ■ True **Default: True** (turned on).
BackupInputFile	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). **Possible values:** ■ False ■ True ■ **Default: False** (turned off).
BackupOutputFile	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). **Possible values:** ■ False ■ True ■ **Default: False** (turned off).

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\Micro 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\Micro 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. Micro Focus Professional Services can create a Custom Word Document Post Processor for you that matches 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\Micro 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 H
Word Import Pre-Processing

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	If enabled, Word Import Pre-Processing allows list items without content. **Possible values:** - false - true **Default: false** (turned off).
ConvertImages	If enabled, Word Import Pre-Processing converts images in WMF or EMZ format to PNG. **Possible values:** - false - true **Default: true** (turned on).
ConvertWordListsToLists	If enabled, Word Import Pre-Processing converts HTML lists to Word lists. **Possible values:** - false - true **Default: true** (turned on).
CorrectPNGImages	If enabled, Word Import Pre-Processing checks if PNG images are faulty. If possible, a faulty PNG image is fixed. **Possible values:** - false - true **Default: true** (turned on).

Setting	Description
RemoveComments	If enabled, Word Import Pre-Processing removes all comments. **Possible values:** ■ false ■ true **Default: true** (turned on).
RemoveIfEndif	If enabled, Word Import Pre-Processing removes all [if ...] and [endif] tags. **Possible values:** ■ false ■ true **Default: true** (turned on).
RemoveOfficeParagraphs	If enabled, Word Import Pre-Processing removes all O:P tags, preserving the content. **Possible values:** ■ false ■ true **Default: true** (turned on).
RemoveTableSize	If enabled, Word Import Pre-Processing removes the width setting for tables **Possible values:** ■ false ■ true **Default: true** (turned on).
RemoveVfTags	If enabled, Word Import Pre-Processing removes V:F tags and any parent tags in the "V" namespace. **Possible values:** ■ False ■ True **Default: True** (turned on).
RemoveWordSections	If enabled, Word Import Pre-Processing removes any class name starting with WordSection or Section. **Possible values:** ■ false ■ true **Default: true** (turned on).

Setting	Description
ReplaceClassesWithStyles	If enabled, Word Import Pre-Processing replaces classes for HTML tags in the Word document with styles. This setting corresponds with the **ReplaceClassWithStyles** setting in chapter "Selector Settings" on page 532. **Possible values:** ■ false ■ true **Default: true** (turned on).
ReplaceImages	If enabled, Word Import Pre-Processing replaces low-resolution images with their high-resolution counterparts if available. **Possible values:** ■ false ■ true **Default: true** (turned on).

Setting	Description
WordBulletListStyle_L1...9	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. **Possible values:** ■ Bullet_Simple ■ Bullet_Empty ■ Bullet_Square ■ Bullet_Color ■ Bullet_Diamond ■ Bullet_Arrow ■ Bullet_Tick **Defaults:** **WordBulletListStyle_L1: Bullet_Simple** **WordBulletListStyle_L2: Bullet_Empty** **WordBulletListStyle_L3...9: Bullet_Square**
WordNumericListStyle_L1...9	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. **Possible values:** ■ Number_Simple ■ Number_Parenthesis_Closing ■ Number_Parenthesis_Surrounding ■ Number_Abc_Lowercase ■ Number_Abc_Lowercase_Parenthesis_Closing ■ Number_Abc_Uppercase ■ Number_Abc_Uppercase_Parenthesis_Closing ■ Number_Roman_Capital ■ Number_Roman_Lowercase ■ Number_Greek_Lowercase **Defaults:** **WordNumericListStyle_L1: Number_Simple** **WordNumericListStyle_L2: Number_Abc_Lowercase** **WordNumericListStyle_L3...9: Number_Simple**

Setting	Description
CorrectImageSize	If enabled, Word Import Pre-Processing resizes images to fit the page. **Possible values:** ■ False ■ True **Default: True** (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	If configured, Word Import Pre-Processing removes all attributes that match the selectors.
	Default:
	`<RemoveAttributes>`
	`    <Attribute>`
	`      <!--Removes all attributes with a namespace.-->`
	`      <AttributeName>:</AttributeName>`
	`      <AttributeNameComparison>Contains</AttributeNameComparison>`
	`      <AttributeValue />`
	`      <AttributeValueComparison>Equals</AttributeValueComparison>`
	`      <AttributeValueIgnoreCase>false</AttributeValueIgnoreCase>`
	`    </Attribute>`
	`  </RemoveAttributes>`

RemoveClasses	If configured, Word Import Pre-Processing removes all classes (entries from the class attribute) that match the selectors.
	Default:
	`<RemoveClasses>`
	`    <Class>`
	`      <!--Removes all Office Mso classes.-->`
	`      <ClassName>mso</ClassName>`
	`      <ClassNameComparison>StartsWith</ClassNameComparison>`
	`      <ClassNameIgnoreCase>true</ClassNameIgnoreCase>`
	`    </Class>`
	`  </RemoveClasses>`

RemoveStyles	If configured, Word Import Pre-Processing removes all styles (entries from the style attribute) that match the selectors.
	Default:
	`<RemoveStyles>`
	`    <Style>`
	`      <!--Removes all Office Mso styles.-->`
	`      <StyleName>mso</StyleName>`
	`      <StyleNameComparison>StartsWith</StyleNameComparison>`
	`      <StyleValue />`
	`      <StyleValueComparison>Equals</StyleValueComparison>`
	`      <StyleValueIgnoreCase>false</StyleValueIgnoreCase>`
	`    </Style>`
	`  </RemoveStyles>`

Setting	Description

RemoveTags	If configured, Word Import Pre-Processing removes all tags that match the selectors.
	Default:
	<pre><RemoveTags>
	    <Tag>
	    <!--Removes all Office style tags-->
	    <TagName>style</TagName>
	    <TagNameComparison>Equals</
	TagNameComparison>
	    <Attributes />
	    <AttributeSelectionMode>Any</
	AttributeSelectionMode>
	    <Classes />
	    <ClassesSelectionMode>Any</
	ClassesSelectionMode>
	    <Styles />
	    <StylesSelectionMode>Any</
	StylesSelectionMode>
	    <PreserveChildren>true</
	PreserveChildren>
	    <RemoveOnlyIfEmpty>false</
	RemoveOnlyIfEmpty>
	    </Tag>
	    <Tag>
	    <!--Removes all tags with a namespace
	and preserves the child nodes.-->
	    <TagName>:</TagName>
	    <TagNameComparison>Contains</
	TagNameComparison>
	    <Attributes />
	    <AttributeSelectionMode>Any</
	AttributeSelectionMode>
	    <Classes />
	    <ClassesSelectionMode>Any</
	ClassesSelectionMode>
	    <Styles />
	    <StylesSelectionMode>Any</
	StylesSelectionMode>
	    <PreserveChildren>true</
	PreserveChildren>
	    <RemoveOnlyIfEmpty>false</
	RemoveOnlyIfEmpty>
	    </Tag>
	  </RemoveTags></pre>

Setting	Description

ReplaceClassWithStyles	If configured, Word Import Pre-Processing sets styles for the specified all class (entry from the class attribute).
	 The **Mode** setting can have these values:
	
	 ■ Ignore
	 ■ RemoveClassOnly
	 ■ AddDocumentStyleOnly
	 ■ AddDocumentStyleAndRemoveClass
	 ■ AddSpecifiedStyleOnly
	 ■ AddSpecifiedStyleAndRemoveClass
	 ■ AddDocumentStyleOrSpecifiedStyleOnly
	 ■ AddDocumentStyleOrSpecifiedStyleOnlyAndRemoveClass
	
	 Default:
	 `<ReplaceClassWithStyles>`
	 `    <ReplaceClassWithStyle>`
	 `      <TagName />`
	 `      <TagNameComparison>Equals</TagNameComparison>`
	 `      <ClassName>msolistparagraph</ClassName>`
	 `      <ClassNameComparison>StartsWith</ClassNameComparison>`
	 `      <ClassNameIgnoreCase>true</ClassNameIgnoreCase>`
	 `      <Mode>AddDocumentStyleOnly</Mode>`
	 `      <StyleValue />`
	 `    </ReplaceClassWithStyle>`
	 `    <ReplaceClassWithStyle>`
	 `      <TagName />`
	 `      <TagNameComparison>Equals</TagNameComparison>`
	 `      <ClassName>*</ClassName>`
	 `      <ClassNameComparison>Equals</ClassNameComparison>`
	 `      <ClassNameIgnoreCase>false</ClassNameIgnoreCase>`
	 `      <Mode>AddDocumentStyleOnly</Mode>`
	 `      <StyleValue></StyleValue>`
	 `    </ReplaceClassWithStyle>`
	 `  </ReplaceClassWithStyles>`

Appendix I

Automatic Termination of MS Word

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. **Possible values:** Any integer greater than 9. **Default: 60**
PollingIntervalInMinutes	Specifies the time ForceExit checks if the target process has terminated **Possible values:** Any integer greater than 0. **Default: 5**

Appendix J

Configuration and Usage of ServiceHelper.exe

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 if you can restart Tomcat. **Possible values:** True, False **Default: True**
RESTART_TOMCAT_ATTEMPTS	Specifies the number of attempts to restart Tomcat. **Possible values:** 2 or larger integer value **Default: 5**
RESTART_TOMCAT_ATTEMPTS_WAIT_SECONDS	Specifies the time in seconds to wait between Tomcat restart attempts. **Possible values:** 30 or larger integer value **Default: 30**
RESTART_TOMCAT_WAIT_SECONDS	Specifies the time in seconds to allow Tomcat to restart. **Possible values:** 30 or larger integer value **Default: 120**

Setting	Description
SECURITY_PROTOCOL	Specifies the security protocol(s) to use when verifying that Tomcat has restarted successfully. These values must contain the same. **Possible values:** Depends on installed .NET framework version: ■ .NET 4.0: SSL3|TLS ■ .NET 4.5: SSL3|TLS|TLS11|TLS12 ■ .NET 4.8: SSL3|TLS|TLS11|TLS12|TLS13 **Default: SSL3|TLS**
SERVICE_NAME_POOL_MANAGER	Specifies the name of the RM Pool Manager service. Do not modify this value. **Possible values:** RMPoolManager **Default: RMPoolManager**
SERVICE_NAME_TOMCAT	Specifies the name of the Tomcat service. Change this only if you do not use Micro Focus Common Tomcat. **Possible values:** Any string with at least one character **Default: MicroFocusTomcat**
START_SERVICE_WAIT_SECONDS	Specifies the time in seconds to allow a service to start. **Possible values:** 5 or larger integer value **Default: 40**
START_STOP_SERVICE_ATTEMPTS	Specifies the number of attempts to start or stop a service. **Possible values:** 1 or larger integer value **Default: 5**
START_STOP_STOP_SERVICE_ATTEMPTS_WAIT_SECONDS	Specifies the time in seconds to wait between start or stop attempts. **Possible values:** 5 or larger integer value **Default: 40**
STOP_SERVICE_WAIT_SECONDS	Specifies the time in seconds to allow a service to stop. **Possible values:** 5 or larger integer value **Default: 25**
SYSTEMINFO_COMMON_TOOLS_SHOW_PATH	Specifies if the path to Micro Focus Common Tools should be included with the system information file. **Possible values:** True, False **Default: True**

Setting	Description
SYSTEMINFO_COMMON_TOOLS_SHOW_VERSION	Specifies if the Micro Focus Common Tools version should be included with the system information file. **Possible values:** True, False **Default: True**
SYSTEMINFO_DATABASE_SHOW_NAME	Specifies if the database name (e.g. Oracle) should be included with the system information file. **Possible values:** True, False **Default: True**
SYSTEMINFO_DATABASE_SHOW_ODBC_VERSION	Specifies if the version of the ODBC driver should be included with the system information file. **Possible values:** True, False **Default: True**
SYSTEMINFO_DATABASE_SHOW_VERSION	Specifies if the database version should be included with the system information file. **Possible values:** True, False **Default: True**
SYSTEMINFO_MSOFFICE_SHOW_PATH	Specifies if the path to Microsoft Office should be included with the system information file. **Possible values:** True, False **Default: True**
SYSTEMINFO_MSOFFICE_SHOW_VERSION	Specifies if the version of the Microsoft Office should be included with the system information file. **Possible values:** True, False **Default: True**
SYSTEMINFO_OS_SHOW_DOTNET	Specifies if the installed .NET frameworks should be included with the system information file. **Possible values:** True, False **Default: True**
SYSTEMINFO_OS_SHOW_DRIVES	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) **Possible values:** * or valid drive letters **Default: ***
SYSTEMINFO_OS_SHOW_ENVIRONMENT_VARIABLES	Specifies if the environment variables should be included with the system information file. **Possible values:** True, False **Default: True**

Setting	Description
SYSTEMINFO_OS_SHOW_RAM	Specifies if free RAM and total RAM should be included with the system information file. **Possible values:** True, False **Default: True**
SYSTEMINFO_OS_SHOW_VERSION	Specifies if the version of the operating system should be included with the system information file. **Possible values:** True, False **Default: True**
SYSTEMINFO_RM_SHOW_PATH	Specifies if the path to Dimensions RM should be included with the system information file. **Possible values:** True, False **Default: True**
SYSTEMINFO_WEBSERVER_SHOW_NAME	Specifies if the name of the web server (usually Tomcat) should be included with the system information file. **Possible values:** True, False **Default: True**
SYSTEMINFO_WEBSERVER_SHOW_PATH	Specifies if the path to the web server (usually Micro Focus Common Tomcat) should be included with the system information file. **Possible values:** True, False **Default: True**
SYSTEMINFO_WEBSERVER_SHOW_VERSION	Specifies if the web server version should be included with the system information file. **Possible values:** True, False **Default: True**
VALIDATION_URL_FORMAT	Specifies the format of the URL to verify that Tomcat has restarted successfully. Do not modify this value. **Possible values:** {0}:{1}/rtmBrowser/cgi-bin/rtmBrowser.exe **Default: {0}:{1}/rtmBrowser/cgi-bin/rtmBrowser.exe**

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 .

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). 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.

Parameter	Description
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: ■ **Root:** Import into Trusted Root Certificate Authorities keystore ■ **CertificateAuthority:** Import into Intermediate Certificate Authorities keystore
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 Micro Focus Common Tomcat).

Parameter	Description
Action	`RestartTomcatSimple`
OutputFile	Specify the path to the file to receive the restart result as plain text.

ValidationUrl	Specify the validation URL in this format: *protocol*://*server*:*port*/rtmBrowser
	
	Replace the format values like this:
	
	■ **protocol:** must be http or https
	
	■ **server:** The name of the machine. For HTTP, it can be localhost. For HTTPS the name must match the name of the certificate.
	
	■ **port:** The port to use. If you do not need a port when accessing Dimensions RM in the web browser, use these default ports:
	
	  • **For HTTP:** 80
	
	  • **For HTTPS:** 443

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`
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 K

Azure Active Directory

Overview

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. The following chapters describe how to register Dimensions RM as an Azure application and how to retrieve the required values for Dimensions RM from Microsoft Azure. For details how to configure Dimensions RM to use Microsoft Azure as a login source, see chapter "Specifying the Azure AD Configuration" on page 274.

Registering Dimensions RM as Azure Application

Before you begin, ensure that you have the login for the administrative account.

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 **Azure Active Directory 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`
Note that this URI is very similar to the one you 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.

Replace *myserver*, mydomain and *8443* with server name, domain and port of your Dimensions RM installation.

24 Add the following URIs in the same manner as with steps 22 and 23:

- `https://myserver.mydomain:8443/rtmBrowser/auth?saml2`

- `https://myserver.mydomain:8443/rtmBrowser/login.jsp`

- `https://myserver.mydomain:8443/rtmBrowser/cgi-bin/rtmBrowser.exe`

- `https://myserver.mydomain:8443/rtmBrowser/auth?saml2`

25 Select option **ID tokens**.

26 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 chapter "Registering Dimensions RM as Azure Application" on page 550.

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   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.

6   **To retrieve the Trust Certificate, do the following:**

a   Navigate to the following URL: `https://login.microsoftonline.com/{tenant_id}/discovery/keys`.
Replace **`{tenant_id}`** with the ID you retrieved in point 3d.

b   Open Notepad.

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).

Appendix L
Configuring Windows SSO

About Windows SSO

Windows SSO allows users to log-in through the web browser their domain user and without specifying their password. Note that not all web browsers support this feature "out of the box." For client applications, e.g. RM Manage, or RM Import, this is not supported. The best method to configure Windows SSO during the Dimensions RM server setup. However, if you want to switch from local RM user accounts to Windows SSO, execute the steps in the following sections.

Configuring Windows SSO

> **IMPORTANT!** Configuring Windows SSO requires to stop the Micro Focus Common Tomcat and RM Pool Manager services. This means that Dimensions RM will not be available at that time. If other web applications are hosted on Micro Focus Common Tomcat, they will also not be available during the time of the configuration.

To configure Windows SSO, do the following:

1 Start the **Services** panel (e.g. by starting `services.msc`).

2 Stop the **Micro Focus Dimensions RM Pool Manager** service.

3 In Windows Explorer, navigate to **RM_INSTALL\conf**, e.g. `C:\Program Files\Micro Focus\Dimensions 12.10`\RM\conf.

4 If the file `sts.pem` exists, rename or delete it.

5 In Windows Explorer, navigate to **RM_INSTALL\support**, e.g. `C:\Program Files\Micro Focus\Dimensions 12.10`\RM\support.

6 Extract the **Windows SSO.zip** file. The following steps will assume that there will be a directory `Windows SSO` with the extracted content.

7 Copy `Windows SSO`\RM\conf\sts.pem into RM's conf folder, e.g. `C:\Program Files\Micro Focus\Dimensions 12.10`\RM\conf.

8 Copy `Windows SSO`\tomcat\webapps\idp.war into Tomcat's webapps folder, e.g. `C:\Program Files\Micro Focus\Dimensions 12.10`\Common Tools `1.8.6.0\tomcat\9.0\webapps`.

9 Wait for 1-2 minutes as Tomcat will unarchive the idp.war file.

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

11 In Windows explorer, navigate to `webapps\idp\WEB-INF\conf`, e.g. *C:\Program Files\Micro Focus\Dimensions 12.10\Common Tools 1.8.6.0\tomcat\9.0*\webapps\idp\WEB-INF\conf.

12 Open the file `fedsvr-core-config.xml` with a text editor, e.g. Notepad.

13 For the parameter "SecurityTokenService", replace protocol, "localhost", and port to match your environment. Replace "localhost" with the server name.

14 Save the file.

15 In Windows Explorer, navigate to the alfssogatekeeper folder, e.g. `C:\Program Files\Micro Focus\Dimensions 12.10\Common Tools 1.8.6.0\tomcat\9.0\`alfssogatekeeper\conf.

16 In the same folder of the file you just edited (`alfssogatekeeper\conf`), open the file `gatekeeper-services-config.xml` with a text editor, e.g. Notepad.

17 Search for `<URIMatcher requestURI="/vault-server/*"/>`.

18 Before `<URIMatcher requestURI="/vault-server/*"/>`, insert the following URIMatcher entries:

```
<URIMatcher requestURI="/rtmBrowser/rest/admin/servicemgmt/statuscommontomcat"/>
<URIMatcher requestURI="/rtmBrowser/rest/admin/certificateupdate/status"/>
<URIMatcher requestURI="/rtmBrowser/rest/htmlCompare/*"/>
<URIMatcher requestURI="/rtmBrowser/rm/img/*"/>
<URIMatcher requestURI="/rtmBrowser/rm/*.js"/>
<URIMatcher requestURI="/rtmBrowser/rm/*.html"/>
<URIMatcher requestURI="/rtmBrowser/rm/*.css"/>
```

19 Save the file.

20 In the same folder of the file you just edited (`alfssogatekeeper\conf`), rename or delete the following files:

- gatekeeper-core-config.xml
- keystore.jks
- truststore.jks

21 Copy the following files to the `alfssogatekeeper\conf` folder, e.g. `C:\Program Files\Micro Focus\Dimensions 12.10\Common Tools 1.8.6.0\tomcat\9.0\`alfssogatekeeper\conf:

- gatekeeper-core-config.xml
- keystore.jks
- truststore.jks

22 Open the file `gatekeeper-core-config.xml` with a text editor, e.g. Notepad.

23 Replace **http** (with https when using secure connections), **localhost** (with the server name), and **8080** (with the Tomcat port) for the following parameter tags:

- SecurityTokenService
- SecurityTokenServiceExternal
- FederationServerURL

Example URL: *http*s://*myserver*:*8443*/idp/services/Trust

24 Save the file.

25 In Windows Explorer, navigate to Tomcat's conf folder, e.g. *C:\Program Files\Micro Focus\Dimensions 12.10\Common Tools 1.8.6.0\tomcat\9.0*\conf.

26 Open the web.xml file with a text editor, e.g. Notepad.

27 In that file, find "<!-- ======== Start of Serena SSO Gatekeeper Filter Configuration ======== -->".

28 Remove the <!-- tag right before the <filter> tag.

Ensure that the value for gatekeeper.enabled is "true":
<init-param>

<param-name>gatekeeper.enabled</param-name>

<param-value>**true**</param-value>

</init-param>

29 Find "<!-- ========= End of Serena SSO Gatekeeper Filter Configuration ========= -->".

30 Remove --> right after </filter-mapping>.

31 Save the file.

32 Double-click Windows SSO\sso_reg.reg and confirm that you want to make changes to the registry.

33 Start the Registry Editor (regedit.exe) as an administrator and navigate to the following path: HKEY_LOCAL_MACHINE\SOFTWARE\Micro Focus\Dimensions RM\Environment\Default.

  a Double-click **SSO_HOST** to open the **Edit String** dialog and replace "localhost" with the server name.

  b Double-click **SSO_PORT** to open the **Edit String** dialog and replace "8080" with the port you use in Tomcat.

  c Double-click **SSO_TRUST_CERTIFICATE** to open the **Edit String** dialog and set its value to the full path of your sts.pem certificate, e.g. *C:\Program Files\Micro Focus\Dimensions 12.10\RM\conf\sts.pem*.

  d Double-click **SSOServer** to open the **Edit String** dialog and replace the URL with one matching your environment, e.g. https://myserver:8443.

34 Start the following services:

  • Micro Focus Dimensions RM Pool Manager

  • Micro Focus Common Tomcat

35 Configure SSO as a login source as described in chapter "Configuring Login Sources" on page 262.

Index

Symbols

!= constraint 335
= constraint 335

Numerics

2FA 275

A

access rights
    granting 214, 215
    inheriting 217
    revoking 216
accounts, Oracle 49
Acrobat Reader 487
Active Directory 274
Add a Comment dialog box, omitting Role menu
       from 292
administrator, adding to instance 210
Adobe Reader 487
Agile
    creating classes 84
    creating relationships 97
    enabling 98
ALF. See Application Lifecycle Framework
ALM integration 46
alphanumeric attribute 299
Amazon cloud 280
animationspeed Web form option 57, 78
Application Lifecycle Framework (ALF)
    architecture 140
    emitting events 141
    enabling instances 144
    event definition 143
    event emitter 143
    logging 149
    overview 140
    trigger points 142
    Web services 143
attribute constraints 361
attributes
    adding 317
    alphanumeric 299
    class 291
    copying 319

Created by 298
    date 300
    defining 317
    deleting 320
    description 236, 326
    file attachment 300
    for specific classes 292
    group 301
    Initial Created by 298
    list 305
    naming 29
    non-unique names 236
    numeric 312
    overview 28
    PUID 316
    rqmt ID 316
    text 313
    title 236, 326
    URL 313
audit trail 39
authenticator app 275
Azure 274
    configure login page 391
    registering 550
    retrieving configuration data 551

B

backing up
    193
    encrypted passwords 190, 191, 192, 193
    instance 175
    legacy mode 191
    normal mode 190
baselines
    setting link options 199
Branching
    creating classes 100

C

cardinality 333
categories
    assigning permissions 218
    naming 29
    overview 38
certificates

W