

CA Role & Compliance Manager

Portal User Guide

r12.5 SP2



This documentation and any related computer software help programs (hereinafter referred to as the "Documentation") are for your informational purposes only and are subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be used or disclosed by you except as may be permitted in a separate confidentiality agreement between you and CA.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO THE END USER OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with "Restricted Rights." Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Copyright © 2010 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Contact CA

Contact Technical Support

For your convenience, CA provides one site where you can access the information you need for your Home Office, Small Business, and Enterprise CA products. At <http://ca.com/support>, you can access the following:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Provide Feedback

If you have comments or questions about CA product documentation, you can send a message to techpubs@ca.com.

If you would like to provide feedback about CA product documentation, complete our short [customer survey](#), which is also available on the CA Support website, found at <http://ca.com/docs>.

CA Product References

This document references the following CA products:

- CA Role & Compliance Manager (CA RCM)
- CA Identity Manager
- CA SiteMinder
- CA Enterprise Log Manager
- CA Service Desk Manager

Contents

Chapter 1: Introduction	11
About This Guide	11
Audience	11
Typical Processes	12
Chapter 2: Using The CA RCM Portal Interface	15
Open the CA RCM Portal	15
User Interface	16
Filter a Data Table	16
User Interface for Non-Administrators	17
Administrator View / User View	17
Language Support	18
Chapter 3: Getting Started	19
Introducing Entities and Links	19
Step 1: Creating a Universe	20
Step 2: Create Import Connectors	21
Step 3: Import Entity Data	21
Step 4: Generating Master/Model Configurations	22
Step 5: Creating a Campaign	22
Step 6: Exporting Entity Data	22
Chapter 4: Using Tickets and the Inbox	23
Tasks and Tickets	23
Inbox Views	23
Search the Inbox	25
Ticket State	27
Ticket Status	28
Ticket Priority	28
Ticket Severity	29
General Approval Ticket Operations	29
Approve	31
Reject	31
Add Comment	32
Add Attachment	33
View Transaction Log	34

View [Entity]	34
Consult	35
View Consult Results	36
Escalate	37
Delegate	38

Chapter 5: Running Certification Campaigns **41**

Certification Campaigns	41
How to Use Campaigns	42
Types of Campaigns	43
Entity Certification Campaigns	43
Recertification Campaigns	44
Define and Launch a Campaign	46
Basic Information Screen	48
Filter Screen	49
Clone the Active Model Configuration for a Campaign	50
What You Can Do During a Campaign	52
Review and Certify Links	53
Reassign Links to Another Reviewer	54
Attach a Comment, File, or Link	55
Customize Ticket Tables	56
Monitor Campaign Progress	58
Define and Send Escalation Emails	58
Suspend and Restart a Certification Campaign	59
Initiate the Approval Phase of a Campaign	59
Certification Decisions	60
Certification and Approval Stages of a Campaign	62
How CA RCM Assigns Certifiers	63
Immediately Invoke Approval Processes	69
Bypass Approval Processes for a Campaign	69
Audit Card Violations in a Campaign	70
How Campaigns Apply Pre-approved Violations	71
The Scope of a Campaign	71
Attribute Value Filters	71
Link Type Filters	72
Audit Card Filters	73
Previously Reviewed Links	73
Updated Links	73
Usage Information from CA Enterprise Log Manager in a Campaign	74
DNA-based Approval Process	74
How to Upgrade Campaigns from Earlier Versions	75

Chapter 6: Using Dashboards	77
Configuration Dashboard	78
Audit Card Dashboard	79
Compliance Dashboard	79
Roles Coverage Dashboard	79
Certification Dashboard	80
Chapter 7: Running Self-Service Tasks	81
General Self-Service Functions	83
Test Compliance	83
Suggesting Entities	84
Manage My Team's Role Assignments	87
General Section (MMT-Role Screen)	88
Users Table (MMT-Role Screen)	89
Currently Enrolled Roles Table (Manage My Roles Screen)	90
Other Roles Table (MMT-Role Screen)	92
Manage My Role Assignments	94
General Section (Manage My Roles Screen)	95
Currently Enrolled Roles Table (Manage My Role Screen)	96
Other Roles Table (Manage My Role Screen)	97
Manage My Team's Resources	99
General Section (MMT-Resources Screen)	100
Users Table (MMT-Resources Screen)	101
Currently Enrolled Resources Table (Manage My Roles Screen)	102
Other Resources Table (MMT-Resources Screen)	104
Manage My Resources	106
General Section (Manage My Resources Screen)	107
Currently Enrolled Resources Table (Manage My Resources Screen)	108
Other Resources Table (Manage My Resources Screen)	108
Defining a New Role	111
Request New Role Definition Screen	111
Definitions for Role Name [New Role Name]	115
Updating Role Definitions	117
Introducing the Requests Table	118
Chapter 8: Role Definition Tickets	121
Role Definition Approval Root Ticket	125
Approval Root Ticket General Functions (Role Definition)	126
Approval Root Ticket Advanced Functions (Role Definition)	127
Role Definition Main Request Parent Ticket	128
Main Parent Ticket General Functions (Role Definition)	130

Main Parent Ticket Details Section	130
Main Parent Ticket Advanced Functions (Role Definition)	131
Add New Role Ticket Tree	133
Select Accountable Ticket (Add New Role)	135
Role Approver Ticket (Add Role)	139
Self-Service Request New Role Parent Ticket	142
Self-Service Request New Role Approver Ticket	145
Update Role Ticket Tree	147
Self-Service Request Update Role Parent Ticket	149
Self-Service Request Update Role Approver Ticket	151

Chapter 9: Entity Browser **155**

User, Role, and Resource Details	156
Modify the Organization Chart	157

Chapter 10: How to Generate Reports **159**

Report Types	160
Parameters and Filters for Report Generation	161
Display a Report's Index	164
Change Report Parameters	164
Export a Report to a File	164
Print a Report	165

Chapter 11: Editing Business Process Rules **167**

Business Process Rule Concepts	167
How to Work with Business Policies in the CA RCM Portal	168
Run Business Policy Files from the CA RCM Portal	168
Create a Business Policy File from the CA RCM Portal	169
Edit a Business Policy File from the CA RCM Portal	170
How to Create and Edit Business Policy Rules in the CA RCM Portal	171

Chapter 12: Using Administration Functions **177**

Universe Settings	177
Work with Universe Settings	178
Customize Tables for a Universe	180
User Account Information	181
How to Use Data from CA Enterprise Log Manager	184
Pre-Approved Violations	191
Import and Export Connectors	194
CA RCM Connectors	196

How to Define Connectors in the CA RCM Portal	197
Define an Import Connector	198
Define an Export Connector	201
Run or Schedule a Connector Job	203
Import and Export Tickets	205
How to Define and Run a Multi-Import Job	206
Job Scheduling	209
Run or Schedule a Job on the CA RCM Portal	209
The Jobs Table	210
Help Desk Integration	211
Set Properties for Help Desk Integration	211
Import Help Desk User Information to the eurekify.udb	213
The Transaction Log	214
Track Portal Usage in the Transaction Log	216
Cache Manipulation	217
Load Cache	218
Clear the Cache	218
Repair CA RCM Configuration, User, and Resource Files	218
Purging Data	219
Purge Selected Documents	220
Purge Data by Date	221
Purge Portal Users from the Permissions Configuration	222
Properties Settings	224
Access the Common Properties Settings Page	225
Creating a New Property Key	226
Editing a Property Key	227
CA RCM Configuration Settings	228
RACI Operations	229
Create RACI	229
Synchronize RACI	230
TMS Administration	231
System Checkup	231
How to Extract CA RCM Data	232
How to Enable the External Report Database	233
Create a Data Extraction Profile	234
Run or Schedule a Data Extraction Job	234
Track Data Extraction Jobs	235
Delete Data Extraction Profiles or Data Snapshots	237

Chapter 13: About Security & Permissions **239**

Security	239
Turning Security On/Off	240

Authentication Settings	241
Encryption	241
Permissions	242
CA RCM Configuration Structure	242
Filters	244
Portal Structure (XML)	246
Chapter 14: Troubleshooting	247
Error Messages	247
Duplicating a Configuration	257
Appendix A: CA RCM Properties	259
tms.delegate.filter	259
tms.escalate.filter	260
tms.campaign.[campaign-type].reassign.filter	260
Appendix B: Portal Structure (XML)	261
Sample Portal Structure XML	262
Appendix C: CA RCM Configuration Data Formats	271
Users Database File	271
Resource Database File	272
Configuration File	273
Role Numbering	276
Glossary	277
Index	281

Chapter 1: Introduction

This section contains the following topics:

[About This Guide](#) (see page 11)

[Audience](#) (see page 11)

[Typical Processes](#) (see page 12)

About This Guide

This guide provides an overview and step-by-step instructions on how to use the CA RCM portal. The CA RCM portal is a web based interface that gives users access to the role management and compliance management features of CA RCM.

Audience

This guide is intended for Role Engineers, system administrators and organizational managers who are in charge of granting and certifying entitlements. Role Engineers are typically well-trained professionals, familiar with the target organization. This manual assumes that the Role Engineer has had professional training on CA RCM client tools and is familiar with the CA RCM documentation that accompanied the client tools installation package.

System administrators should be familiar with the CA RCM software, downloading and uploading of users and resources databases, role discovery and audit operations. This guide is also intended for general administrators and organizational managers who are in charge of various processes, and therefore have to access the portal in the course of their daily activities. Other users will have limited access to the CA RCM Portal's options.

Familiarity with the Microsoft operating system and applications and relevant peripheral and remote equipment is also assumed.

More information:

[About Security & Permissions](#) (see page 239)

Typical Processes

The CA RCM Portal provides access to both information and processes necessary for system-wide role management, compliance management, certification campaigns and relevant security management oversight.

The following are the main CA RCM Portal processes:

Ticket Based Task Management

Most business managers and resource owners in the company interact with CA RCM through a ticket based task management system. When users log in to the portal, their Inbox contains tickets for any review and certification tasks that are assigned to them.

Running Campaigns

Campaigns utilize CA RCM's basic auditing tools to run an enterprise certification and attestation process by designated approvers. The purpose of the campaign is to certify that granted privileges comply with the business and regulatory needs, and that they are not over allocated. This process is supported by the CA RCM Audit Card facility which allows the presentation of out-of-pattern and non-compliance information to the approver. The campaign administrator can apply pattern recognition tools and policy enforcement rules to analyze a configuration and run a comprehensive audit. The output of an audit is the Audit Card, which contains a list of all suspicious records and the type of suspicion involved (currently about 50 different types).

Part of the cleansing process and an important step before starting the role engineering process is for business managers (Approvers) to review the access rights. A manager can be in charge of a team of users, one or more roles or one or more resources. In a business with over 1000 users, the help of the managers is required to speed up the cleansing process. Depending on the campaign definitions, the business managers may be required to review the access rights of their employees and/or resources under their jurisdiction, and report the change requests to the CA RCM Administrator. Campaigns are used not only in the enterprise cleansing phase, but also for periodic certification as required by regulation.

Self-Service

Managers can use the CA RCM Portal to manage their team's role definitions and access to corporate resources. Users can also manage their own personal privileges with regard to system roles and resources.

Entity Browser

This browser aids the administrator/business manager who is using the CA RCM Portal in viewing entities (i.e. users; roles; resources) associated with a specific Universe under a selected configuration. The information is displayed in table format. The tables contain basic information for each entity.

Running reports

Provides access to a variety of reports.

Dashboards

Automatically shows users useful statistical information as they go about their tasks.

Administration

Administrators can create a universe, generate import/export connectors and define their scheduling. They can also perform other functions available only to senior administrators.

More information:

[Using The CA RCM Portal Interface](#) (see page 15)

Chapter 2: Using The CA RCM Portal Interface

The user interface, menus and options are fully described in this chapter. Not all users will have full administrative privileges and therefore, not all the described options will be available for all users.

This section contains the following topics:

[Open the CA RCM Portal](#) (see page 15)

[User Interface](#) (see page 16)

[User Interface for Non-Administrators](#) (see page 17)

[Language Support](#) (see page 18)

Open the CA RCM Portal

Once you install and start CA RCM, you can open the web-based interface from a remote computer using the URL for CA RCM portal.

To open the CA RCM Portal

1. Open a web browser and enter *one* of the following URLs:

- To use a non-SSL connection, enter the following URL:

`http://ServerName:Port/eurekify`

- To use an SSL connection, enter the following URL:

`https://ServerName:HTTPSPort/eurekify`

The Login screen opens.

2. Enter your credentials.

Note: Both the User Name and Password are case-sensitive.

3. Click Log In.

The CA RCM portal Home page appears.

More information:

[Using The CA RCM Portal Interface](#) (see page 15)

User Interface

You can use the following general usability features in the screens of the CA RCM portal:

- Autocomplete—in fields that reference field names or values of a data file, the portal completes your typing with matching values from the data file. You can also press the Down Arrow key to scroll through a list of available field values.
- Mandatory fields—fields marked with an orange dot are mandatory. You cannot proceed to the next stage of a process without filling in these fields.
- Customizable Tables—click Customize in the header bar of a table to change the columns shown and the order in which they are displayed. Click a column header to sort the table by the values of that column. You can also use the Records per page drop down to limit or extend the size of a long table.

Filter a Data Table

You can filter the records in a table. When filtering is relevant, a Filter option appears in the header of the table. You can filter the table contents using a combination of criteria.

The filter allows only *AND* statements and is limited to three statements:

- Two are exact statements (Is/contains):
[Selected Field] **Is/contains** [Field Dependent content]
where the content of the drop-down list depends on the field you select
- One filter is an *include* statement :
[Selected Field] **Includes** [Free text]

Note: Sometimes the third filter statement option is the same as the first two.

To filter a data table

1. Click Filter.
The Filter pop-up window appears.
2. Select the fields and values you want to display in the table from the drop-down lists. Use the Includes field to enter a free text filter term.
3. Click OK.
The table displays only records that match the field values that you specified.

User Interface for Non-Administrators

Several types of users connect to the CA RCM portal:

- Administrators and role engineers use CA RCM to model and maintain the data universe. They configure data connectors that update the universe model and export changes in privilege settings to provisioning endpoints. They define and run certification campaigns to verify user privileges.
- Business managers interact with CA RCM primarily as participants in certification campaigns. They can also use the role management features of the portal to change the privileges related to users or resources they manage. All these tasks are supported using a ticket-based task management system.

When users log in to the CA RCM portal, they can access only the portal features that are relevant to them. Business managers can only access their own Inbox, the Role Management area, and other relevant areas of the portal. Administrators can access all areas of the portal. They can define data universes and connectors and create campaigns.

More information:

[About Security & Permissions](#) (see page 239)

Administrator View / User View

The Admin View/User View button allows you to toggle between two views of the Inbox:

User View

The standard Inbox features available to all users (dependent on their permissions).

Admin View

Allows you to view all the campaign tickets in the system, even those that were created by other managers.

The Admin View option is only available to the super administrator. The buttons will only appear for users that are linked to the role defined in `eurekify.properties` as the system administrator role. The default, out-of-the-box option is:

```
sage.admin.role=CA RCM Admin Role
```

More information:

[About Security & Permissions](#) (see page 239)

[CA RCM Properties](#) (see page 259)

Language Support

The CA RCM portal interface appears in the language you selected during installation. To help ensure that text direction, date formats, and other aspects of the user interface conform to the selected language, set the language of your browser to the language of the interface.

Chapter 3: Getting Started

This chapter describes the order of procedures to be carried out when running the CA RCM Portal on a system whose user, role and resource data has not yet been downloaded by the CA RCM system. The step-by-step details, for each step in the procedures mentioned here, are described in later chapters.

This section contains the following topics:

[Introducing Entities and Links](#) (see page 19)

[Step 1: Creating a Universe](#) (see page 20)

[Step 2: Create Import Connectors](#) (see page 21)

[Step 3: Import Entity Data](#) (see page 21)

[Step 4: Generating Master/Model Configurations](#) (see page 22)

[Step 5: Creating a Campaign](#) (see page 22)

[Step 6: Exporting Entity Data](#) (see page 22)

Introducing Entities and Links

Throughout this guide, we describe entities and links. Entity refers to the users, roles, and resources that are the subject of the security review, certification, and attestation processes that are run using the CA RCM Portal. A link is a connection between two or more entities.

The CA RCM Portal recognizes the following three categories of links:

Direct links

An uninterrupted connection between two entities. For example, a user to resource link.

Indirect links

A non-direct connection between two or more entities. For example, a user links to a specific role and the role links to a specific resource. The link between the user and the resource is an indirect link.

Dual links

Specifies when both a direct link and an indirect link exist. For example, a user links directly to a specific resource, and at the same time the user links to a role that links to the same resource.

Direct links and dual links are examined during the various review processes, for example, during campaigns, or when assigning a role to a specific corporate team. Indirect links are listed for completeness, but are not subject to the review process.

The following is a list of possible direct links between entities:

- user-role
- user-resource
- role-resource
- role-role (hierarchy)

Step 1: Creating a Universe

A universe is a virtual location that encompasses the data collected from the enterprise security and identity management systems. This data is stored in the CA RCM configuration files. A universe consists of a specific pair of master-model configurations, enabling tracking of differences between the real-world configuration imported from the system (master) and the desired configuration generated after a campaign (model).

You need the following information to create a universe:

- Master configuration file name and path
- Model configuration file name and path
- (Optional) Approved Audit Card
- Audit Settings file name and path
- Names of the fields (in the configuration files) that contain the following information:
 - Login
 - Email
 - User manager
 - Role manager
 - Resource manager

Note: You can provide names of configuration files that do not yet exist. Because you do not have the field names, you create the master/model configuration files later and then update the universe with the correct field names.

More information:

[Universe Settings](#) (see page 177)

Step 2: Create Import Connectors

After defining the universe that you intend to audit, import user and user privileges from various endpoints. This process requires you to define import connectors.

Importing refers to downloading user, resource, and role information from an endpoint system. Exporting refers to uploading changes in user, resource, and role information that is generated after an audit.

Note: For more information about connectors, see the Using Administration Functions section of this guide.

More information:

[Import and Export Connectors](#) (see page 194)

Step 3: Import Entity Data

“Import” refers to downloading the system’s current user, resource and role (when available) configuration data. You can use the import-connector that you created in Step 2 to download the entity data from the enterprise endpoints.

You can also use the Import option on the CA RCM Data Management menu bar to import the entity data (see Chapter 2: in the *Data Management Guide*).

The output of the import process is a Sage configuration document (.cfg file), which sets the stage for the role discovery process.

Step 4: Generating Master/Model Configurations

When you created a Universe, you provided the names of two configuration files, one was the master configuration file and the other was the model configuration file. The master configuration file contains the data imported from endpoint systems. The model configuration file is initially a copy of this data, which is processed and updated as the role modeling and audit processes proceed.

Use the instructions in [Appendix A: Duplicating a Configuration](#) (see page 257), to generate the master and model configuration files using the CA RCM DNA module. If necessary, edit the universe so that the listed master and model configurations match the ones you generated.

After you create or edit a universe, enter the users associated with the universe into the CA RCM permissions configuration, so that the users will have access to the CA RCM Portal. Typically this process involves RACI synchronization to assign each user the rights they need on the portal.

More information:

[CA RCM Configuration Settings](#) (see page 228)

[RACI Operations](#) (see page 229)

Step 5: Creating a Campaign

A campaign is an audit process which entails reviewing links between users, roles, and resources. Managers in charge of various entities are notified that a campaign has begun. The tasks assigned during the campaign are presented to the campaign owner and approvers as tickets. The tickets include information necessary to review, and approve or reject the task.

Step 6: Exporting Entity Data

The differences between the original real-world configuration that was imported from system endpoints (Master) and the updated and corrected configuration that has gone through an auditing process (Model) are exported to the original endpoints, thus updating the corporate and platform user and user privileges information so that they are now in compliance with corporate policies and regulations.

More information:

[Define an Export Connector](#) (see page 201)

Chapter 4: Using Tickets and the Inbox

This section contains the following topics:

[Tasks and Tickets](#) (see page 23)

[Inbox Views](#) (see page 23)

[Search the Inbox](#) (see page 25)

[Ticket State](#) (see page 27)

[Ticket Status](#) (see page 28)

[Ticket Priority](#) (see page 28)

[Ticket Severity](#) (see page 29)

[General Approval Ticket Operations](#) (see page 29)

Tasks and Tickets

Role based management of user privileges involves managers and resource owners throughout the company. For example, administrators use CA RCM to run a certification campaign, business managers must review the privileges of their workers. Similarly, if a manager requests access to a resource for one of their workers, the owner of that resource must review and approve the privilege.

CA RCM uses a ticket based system to implement these tasks. Managers in the company receive email notifications when CA RCM needs them to certify existing privileges or approve changes to privileges or roles. When they log in to the CA RCM portal, these tasks are packaged as tickets in their Inbox.

In most cases, managers complete the task by interacting with the ticket. For example, each business manager participating in a certification campaign receives a personalized ticket containing the privileges and links that they must review. They indicate their review decisions by clicking check boxes in the screens of the ticket.

The CA RCM server creates and maintains an Inbox for every user in the Permissions configuration file. This configuration file defines user accounts on the CA RCM portal.

Inbox Views

The Inbox your tickets in table format. The Inbox menu provides the following predefined filtered views:

Open/New/Done

Presents tickets whose state is Open, New or Done.

New Tickets

Presents new tickets.

Overdue Tickets

Presents the tickets whose end date has already passed.

Approver Tickets

Presents the current user's Approver tickets. This is most relevant to Administrators who can view their own tickets, and the Approver tickets associated with campaigns they own.

Campaign Tickets

Presents Campaign tickets.

Archived Tickets

Presents tickets that were sent to be archived.

The columns of the inbox are customizable.

The inbox shows your own tickets and tickets that were generated by you, even though they have a different owner. Tickets are grouped in tree structures based on the certification campaign or administrative process to which they are related.

Administrators see their own tickets, and also tickets assigned to their team(s) and tickets of campaigns they created. Administrators can use the following option to control their Inbox display:

Admin View / User View

Specifies whether the Inbox shows all tickets relevant to an administrator, or just the tickets relating to their own tasks, as for a normal user. These options function as a toggling pair in the Inbox screen.

More information:

[General Approval Ticket Operations](#) (see page 29)

Search the Inbox

Besides the basic filtering done by the Inbox menu options, you can search for a ticket that matches a specific query. The search is performed on the tickets in the current table.

The query can include one or more filter statements. Each rule consists of the following fields:

Field	Description
[Column name]	This drop-down box provides a list of possible columns. You can select any column that appears in the drop-down list, even if the column is not currently visible in the Inbox.
Filter functions	The following filtering functions are available: <ul style="list-style-type: none">■ Equal■ Greater■ Less■ Between■ In■ Is null■ Is not null■ Not equal■ Like
[Item]	Based on the column name, you can select an item from a drop-down list, or enter free text. For example: <ul style="list-style-type: none">■ If the column name is Status, you can select Pending Action from the drop-down list.■ If the column name is Owner, you can enter free text.

The Search Ticket window provides two functions:

Add Condition

Allows you to add an additional filter rule to the search criteria. The dependency between the rules is that all the criteria must be met (AND) in order for a record to be located.

Delete

Allows you to delete the filter rule located next to the button.

Note: The search only checks the top-most ticket in each ticket tree within the Inbox.

To search the Inbox

1. Click Search on the Inbox menu bar.
The Search Ticket screen opens in a separate browser window.
2. Create a rule by making selections from the search fields.
Click Add Condition to add additional rules.
3. Click OK when you are satisfied with the query you have generated.
4. If there are tickets that match your filter statements, they appear in the ticket table. The Clear Filter button is added to the Inbox's menu bar.
5. Click Clear Filter to return to the original filtered (by Inbox menu options) ticket table.

Ticket State

The following lists the various possible ticket states:

New

Indicates a new ticket that hasn't yet been opened by the user.

Open

Indicates that the ticket has been opened.

Hidden

Indicates a ticket that is not visible to its assigned user.

Done

Indicates that the action referred to by the ticket has been completed.

Archived

Indicates that the ticket has been archived.

Canceled

Indicates that the ticket was canceled.

Ticket Status

The following lists the various possible ticket statuses:

Active

Indicates that the ticket is active.

Completed

Indicates that the links listed in the ticket have been audited.

Delegated

Indicates that the ticket was delegated by a more-junior manager.

Done

Indicates that the ticket's job has been completed.

Escalated

Indicates that the ticket was reassigned to a more-senior manager.

In Progress

Indicates that the ticket is being processed.

None

Indicates that there is an error related to this ticket, so it cannot be processed.

Pending Action

Indicates that the ticket is waiting for a user to take action.

Reassigned

Indicates that a link approval has been sent to another entity manager.

Rejected

Indicates that a link has been rejected.

Ticket Priority

Tickets can display one of the following priority designations:

- Low
- Normal
- Rush
- Critical

Ticket Severity

Tickets can display one of the following severity designations:

- Minimal
- Medium
- Serious
- Urgent
- Critical

General Approval Ticket Operations

CA RCM includes function buttons in ticket layouts. Depending on the purpose of the ticket, the following operations are available to you in tickets:

Note: This list describes options available to participants in the approval phase of a campaign, or in role management processes. In tickets for the initial review phase of [certification campaigns](#) (see page 41), many of the operations listed below are represented by icons.

Close

Closes the ticket.

Save

Saves the changes made to the ticket.

Delegate

Transfers the ticket to another manager.

Escalate

Transfers the ticket to a higher-level manager.

Acknowledge

Archives the ticket.

Add Comment

Adds a comment to reviewed entities in a ticket.

Add Attachment

Adds an attachment or URL to reviewed entities in a ticket.

View Transaction Log

Displays a history of actions related to the ticket.

View Parent

Opens the parent ticket of the current ticket.

View Children

Opens the child tickets of the current ticket.

View [Entity]

Opens an entity browser window with details of the entity under review.

View Initiators

Displays a list of the creators and owners of the current ticket.

Save and Reassign

Saves changes to the ticket and lets you select a new owner for tasks that you reassigned.

Hide Selected/Show All

Hides entities whose links have already been reviewed. When there are hidden entries, the Show All button appears.

Note: A sub-group of review tasks is hidden only if all tasks of the sub-group are complete. Partially complete sub-groups are not hidden.

Consult/View Consult Results

Sends a copy of the specified review tasks to other users to see how they would decide. When you have initiated consultation, the View Consult Results button appears.

Start Process

Activates approval tasks in a certification campaign or role management process.

Cancel Process

Stops approval tasks in a certification campaign or role management process.

View Statistics

Displays the status of all the child tickets of the current ticket.

Check Violations

Displays the business process rules or statistical measures that the links under review violate.

More information:

[Administrator View / User View](#) (see page 17)

Approve

As an approver, it is your task to approve or reject the request to delete a link between two entities. When you choose to approve such a request, click Approve and a Confirmation pop-up window opens.

Click Yes and the Executing bar appears. When done, the approver ticket's status is Approved and the ticket is archived. The user whose privileges were altered by this decision receives a ticket and email notifying him of the change. In the case of a role-resource or role-role (hierarchy) link, the designated role/resource managers are informed.

Reject

As an approver, it is your task to approve or reject the request to delete a link between two entities. When you choose to reject such a request, click Reject and a Confirmation pop-up window opens.

Click Yes and the Executing bar appears. When done, the approver ticket's status is Rejected and the ticket is archived. The user whose privileges were altered by this decision receives a ticket and email notifying him of the change. In the case of a role-resource or role-role (hierarchy) link, the designated role/resource managers are informed.

Add Comment

Using this function you can add specific comments in free style text This is in addition to system comments that may be added during a ticket's life cycle, for example, during a campaign, a comment is added when a campaign is delegated.

All the comments appear in the Comments table.

The Comments table provides the following information:

Received

Provides the date when the comment was generated.

Owner

The name of the user who generated the comment.

Note: The content of the comment.

Next to each comment, you can see an **X**. Click **X** to delete the comment.

The Add Comment screen contains two fields:

Owner

Lists the name of the note owner

Note: Free style text.

To add a comment

1. Click Add Comment.
The Add Comment screen opens.
2. Enter the comment you want to make in the Note field.
3. Click Save.

The Executing bar appears. The new comment appears in the Ticket Properties Form's Comment table.

Add Attachment

An advanced ticket feature that allows you to attach a file or URL to a specific ticket. Next to the listed attachment(s) you can see an **X**. Click **X** to delete the attachment.

The Add Attachment screen contains three fields:

Name

Lists the attachment name. When the attachment is a file, the file name is listed.

URL

The URL to be listed as an attachment.

File

The file to be attached. You can use the Browse button to locate the file.

To add an attachment

1. Click Add Attachment.
The Add Attachment screen opens.
2. To link to a URL: enter the URL in the URL text box.
3. To attach a file: enter the file name or locate it using the Browse option.
4. Click Save.

The Executing bar appears. The URL/file appears in the Ticket Properties Form under Attachments. You can open the URL or file by clicking on the provided link.

View Transaction Log

The transaction log provides a history of the ticket-related actions executed since the creation of the ticket.

The View Transaction Log table provides the following information:

Date

The date when the transaction took places.

User

Full user name.

Action

The type of action taken.

Message

A full description of the action taken.

To view the campaign's transaction log

1. Click Advanced at the bottom of the Ticket Properties Form.
2. Click View Transaction Log.

The View Transaction Log table opens in a separate browser window.

3. Click Close to close the pop-up.

View [Entity]

The purpose of the Approval Process is to review the rejected links recorded during the original campaign run. This task is performed by the various entity managers. An important aid to this is the ability to view the link's entity cards during the approval process. View [Entity] opens the entity's card in a separate browser window.

The Approval Process tickets that provide this option (Rejected-Link Parent and Approver tickets) provide two action buttons-one for each side of the link. Therefore, if the rejected link being reviewed is a user-role link, the advanced function buttons will be View User and View Role.

Click View User/View Resource/View Role to see the entity's card in a separate browser window.

Consult

You can use the Consult utility to send a request for a consult concerning a link that you are reviewing during an Approval Process. You can consult more than one user at a time. You also don't have to wait for an answer to your request before you actually approve or reject the link listed in the Approver ticket. This feature is particularly useful when you are facing a deadline.

When you click Consult the Find Users screen opens in a separate browser window.

The Find Consult Users screen is divided into two sections:

The filter

Located in the window's header. The filter lets you narrow down the list of proposed approvers.

The proposed users

This table presents a pre-filtered list of users who can receive the request to provide a consultation. This list can be filtered to aid in finding a specific user.

You can select more than one user to consult with. After selecting the first user to consult with, the Consult button toggles to become the Consult More button. The View Consult Results is added to the ticket's Advanced functions.

Consulting another user generates a ticket of the same type as the source Approver ticket. The approver who made the consultation request can see a copy of the consultant tickets, listed as leaves below the original Approver ticket in the Inbox.

The consult ticket that is generated is sent to each consultant's Inbox.

The ticket itself is identical to the original Approver ticket (Delete Link Entity1-Entity2) except it has a new Ticket ID and the General functions are limited.

The options Approve and Reject have the following meaning:

Approve

Approve the request to delete the specified link.

Reject

Reject the request to delete the specified link.

Click View Parent to see the ticket from which the consultation request originated (all functions disabled).

When you approve or reject the link, the consultation ticket is archived.

You can check this ticket's Transaction Log to view what decision was made in this case.

To consult on a ticket

1. Click Consult in the ticket's Ticket Properties Form.

The Find Users screen opens in a separate browser window.

2. Select one or more names from the list. You can use the filter option to reduce the number of records listed in the table.
3. Click OK.

The Executing bar appears. A new ticket is generated for each consultant listed. The new ticket(s) will now appear in the consultant's Inbox.

4. Click View Consult Results to view the results of the consultation.

More information:

[Filter a Data Table](#) (see page 16)

View Consult Results

When an Approver sends a request for a consult during an Approval Process, the View Consult Results button is added to the ticket's Advanced function buttons. When you click this button, you open the View Consult Results window in a separate browser window. Click Close to close the window.

You can use this utility to see what the consultation results are. If at the time of the viewing no answers are available, the screen will list this data as follows:

The View Consult Results table has two columns:

Action

The action was taken by the consulting parties.

Counter

The number of consultants who responded in this manner.

Over time, as the various users respond to the request for a consultation by approving the request to delete a link or rejecting it, the table shows the various responses.

Click View Consult Results to view the View Consult Results screen in a separate browser window. Click Close to close the browser window.

Escalate

This function lets you transfer the selected ticket to a more senior manager. Once you have transferred the selected ticket to the new ticket owner, the original ticket is archived and will no longer appear in your list of active tickets. Only the current ticket owner can escalate a ticket.

When a ticket is escalated, a new ticket is generated with the new owner listed in the Owner field and the manager who escalated the ticket(s) is listed in the Previous Owner field.

A comment is generated stating that the ticket has been Escalated to [current owner]. This comment appears in both the old ticket and in the new ticket.

When viewed in the original ticket owner's Archive screen (Inbox, Archived Tickets) the old ticket and the new ticket create a hierarchal tree in which the original ticket (the Status is set to Escalated) is the root ticket and the new ticket is the next node.

When the escalated ticket is viewed in the Approval Process owner's Inbox (when applicable), the old ticket and the new ticket create a new sub-tree within the original Approval Process tree, in which the original ticket (Status is set to Escalated) is the parent ticket.

If the ticket that you chose to transfer is a parent ticket, having other tickets located below it in the specific Approval Process ticket tree, then the complete sub-tree will now be listed in the new owner's Inbox.

If you choose to escalate an Approval Process root ticket, the whole tree will now be visible in the new owner's Inbox.

To escalate a ticket, you have to select a user from the list of appropriate users.

The Find Escalate Users screen is divided into two sections:

The filter

Located in the window's header. The filter lets you narrow down the list of proposed approvers.

The proposed users

This table presents a pre-filtered list of users who can receive the escalated approval task(s). This list can be filtered to aid in finding a specific user.

The names listed in the proposed users list are governed by several default property filters of the type:

`tms.escalate.filter`

To escalate a ticket

1. Click Escalate in the ticket's Ticket Properties Form.

The Find Escalate Users screen opens.

2. Select a name from the list. You can use the filter option to reduce the number of records listed in the table.
3. Click OK.

The Executing bar appears. The original ticket is archived and its status is set to Escalated. A new ticket is generated. The ticket appears in the target user's Inbox.

More information:

[Add Comment](#) (see page 32)

[Filter a Data Table](#) (see page 16)

[CA RCM Properties](#) (see page 259)

Delegate

This function allows you to transfer the selected a ticket to another user. Once you have transferred the selected ticket to the new ticket owner, the original ticket is archived and will no longer appear in your list of active tickets. Only the current ticket owner can delegate a ticket.

When a ticket is delegated, a new ticket is generated with the new owner listed in the Owner field and the manager who delegated the ticket is listed in the Previous Owner field.

A comment is generated stating that the campaign has been Delegated to [current owner]. This comment appears in both the old root-ticket and in the new root-ticket.

When viewed in the original ticket owner's Archive screen (Inbox, Archived Tickets) the old ticket and the new ticket create a hierarchal tree in which the original ticket (the Status is set to Delegated) is the root ticket and the new ticket is the next node.

When the delegated ticket is viewed in the Approval Process owner's Inbox (when applicable), the old ticket and the new ticket create a new sub-tree within the original Approval Process tree, in which the original ticket (Status is set to Delegated) is the parent ticket.

If the ticket that you chose to transfer is a parent ticket, having other tickets located below it in the specific Approval Process ticket tree, then the complete sub-tree will now be listed in the new ticket owner's Inbox.

If you choose to delegate an Approval Process root ticket, the whole tree will now be visible in the new owner's Inbox.

To delegate a ticket, you have to select a user from the list of appropriate users.

The Find Delegate Users window is divided into two sections:

The filter

Located in the window's header. The filter lets you narrow down the list of proposed approvers.

The proposed users

This table presents a pre-filtered list of users who can receive the delegated approval task(s). This list can be filtered to aid in finding a specific user.

The names listed in the proposed approvers list are governed by several default property filters of the type:

`trns.delegate.filter`

To delegate a ticket

1. Click Delegate in the ticket's Ticket Properties Form.

The Find Delegate Users screen opens.

2. Select a name from the list. You can use the filter option to reduce the number of records listed in the table.
3. Click OK.

The Executing bar appears. The original ticket is archived and its status is set to Delegated. A new ticket is generated. The ticket appears in the target user's Inbox.

More information:

[Add Comment](#) (see page 32)

[Filter a Data Table](#) (see page 16)

[CA RCM Properties](#) (see page 259)

Chapter 5: Running Certification Campaigns

This section contains the following topics:

[Certification Campaigns](#) (see page 41)

[How to Use Campaigns](#) (see page 42)

[Types of Campaigns](#) (see page 43)

[Define and Launch a Campaign](#) (see page 46)

[What You Can Do During a Campaign](#) (see page 52)

[Certification and Approval Stages of a Campaign](#) (see page 62)

[Audit Card Violations in a Campaign](#) (see page 70)

[The Scope of a Campaign](#) (see page 71)

[Usage Information from CA Enterprise Log Manager in a Campaign](#) (see page 74)

[DNA-based Approval Process](#) (see page 74)

[How to Upgrade Campaigns from Earlier Versions](#) (see page 75)

Certification Campaigns

Certification campaigns open the role hierarchy, user privileges, and business rules you define in CA RCM to review. When you initiate a certification campaign, CA RCM automatically invites managers to review and certify the access privileges of the users or resources they administer. CA RCM provides tools to customize, track, and manage the certification process, and to implement changes indicated by reviewers.

Certification campaigns support the following business cases:

- Confirm data security compliance—Where there is a legal requirement to demonstrate data security measures, certification campaigns document periodic review of access to data by employees.
- Refine Role-based Access Control—Review of the resources and child roles included in each role confirms that the role hierarchy suits actual patterns of usage, and that role definitions are useful.

How to Use Campaigns

You can customize certification processes to support many business needs. The basic campaign process follows this general pattern:

1. A role engineer or high-level administrator defines the campaign in CA RCM based on business needs. The campaign owner specifies the following information for the campaign:
 - The universe on which the campaign is based, and additional data such as audit cards and member lists that the campaign uses.
 - Filters that reduce the scope of the campaign to a subset of entities or links in the configuration.
 - How the campaign identifies certifiers for each entity under review.
 - How to handle changes made by reviewers.CA RCM creates the campaign, and automatically assigns the entities and links under review to managers and administrators in the enterprise.
2. When the campaign launches, CA RCM sends these managers email invitations that include links to the CA RCM server. On the server, managers use a ticket-based task management system to review and certify the entities and links assigned to them.
3. When certifiers reject existing links or suggest new links, the configuration must be changed. CA RCM contacts the managers of the entities involved, and requests approval of the change. These approval tasks are also managed using the ticket-based system. Approved changes are then implemented in the target configuration.

Example: Certify User Privileges Following an Acquisition

Companies commonly use certification campaigns to review and certify the roles and resources assigned to each user. In this example, new users and resources were added to the CA RCM model configuration following an acquisition. Administrators run a certification campaign to verify the privileges assigned to these new users.

The stages of the campaign are as follows:

1. The role engineer creates a campaign that certifies user entities and their links. The role engineer defines user attribute filters that limit the scope of the campaign to the new employees. A member list maps managers to the new users and resources.

2. Each manager reviews the privileges assigned to their workers. Bob Smith reviews the privileges given to Hector Torres, and suggests access to a database that Hector needs in his new position.
3. CA RCM sends an email to Deepak Chamarti, the owner of the database. Deepak approves the change, and CA RCM updates the configuration. Hector Torres now can access the database.

Types of Campaigns

Certification campaigns support various business needs. CA RCM provides the following types of certification campaigns:

- Entity Certification—Certify the links associated with selected users, role, or resource entities.
- Recertification—Repeat the certification process based on a previous campaign.

Entity Certification Campaigns

Entity certification campaigns let reviewers examine and certify links between user, role, and resource entities in a CA RCM configuration.

Each entity certification campaign focuses on one type of entity, and its links. The following campaigns are possible:

- User-centric campaigns certify the roles and resources linked to each user. These links define the privileges assigned to each user. Typically, managers review the privileges of their workers.

Use this type of campaign to document compliance with legally-mandated data security measures.

- Role-centric campaigns certify the resources, parent or child roles, and users linked to each role. Typically, the owner of each role reviews the links that define their role, and the users who were assigned the role.

Use this type of campaign to maintain the role hierarchy.

- Resource-centric campaigns certify the users and roles that link to each resource. Typically, the administrator of each resource reviews the roles and users that have access to the resource.

To implement an entity certification campaign, select the User Privileges, Role Definitions, or Resource Links option in the Campaign type field of the campaign creation wizard.

Self-Attestation Campaigns

A self-attestation campaign is a user certification campaign in which each user under review certifies their own privileges.

This type of campaign satisfies some legal requirements for data security certification. This type of campaign is also useful during construction of the role hierarchy, and as a starting point for subsequent certification by managers.

Typically, the active configuration is not changed based on self-certification. When you plan your campaign, consider how you want to use the campaign results. If you want to create a configuration file that reflects user changes, create a separate file in which you can implement changes.

To implement a self-attestation campaign, select the Self-Attestation option in the Campaign type field of the campaign creation wizard. The wizard presents options relevant to this type of campaign:

- Because each user is their own reviewer, you cannot assign reviewers based on a member list or RACI configuration. These options are not available in the Reviewers screen of the wizard. However, you can specify a default reviewer for the campaign.
- By default, approval and implementation tasks are aggregated into a second, later phase of the campaign, which you must launch manually from the top-level ticket of the campaign. The Initiate Approvals field of the Execution screen reflects this default setting.

Depending on your business goals, you can export information from the finished campaign as an Audit Card for further processing, or implement changes from the campaign on the target configuration. You can also use the campaign as the basis for a recertification or differential campaign.

Recertification Campaigns

A recertification campaign creates a set of certification tasks based on a previous campaign.

Use this type of campaign when you require multiple reviews before changes are implemented. For example, you can recertify a user self-attestation campaign, with managers instead of workers. The managers can see the results of user self-certification as they perform their review.

To implement a recertification campaign, select the Recertification option in the Campaign type field of the campaign creation wizard. The wizard presents options relevant to this type of campaign:

- The wizard prompts you to specify an existing campaign in the universe. The recertification campaign is based on this previous campaign.
- Because the base set of review tasks is inherited from the previous campaign, you cannot filter included links by entity attributes.
- You can specify which [direct, indirect, or dual links to include](#) (see page 72) in the campaign.
- You can filter included links [by the final state of each review task](#) (see page 73) in the previous campaign.
- Decisions by previous reviewers appear in the History section of review tickets. You can also specify that these decisions are selected by default in the tickets of the new campaign.
- You can have CA RCM suggest new links based on the audit card specified for the campaign.
- You can [update the campaign](#) (see page 73) with links in the configuration that were not included in the previous campaign. An icon indicates new links.
- You cannot [assign reviewers](#) (see page 63) based on a RACI configuration. Instead, you can use a member list, resubmit certification tasks to the previous reviewer, or submit each task to the manager of the previous reviewer.
- By default, approval and implementation tasks are aggregated into a second, later phase of the campaign, which you must launch manually from the top-level ticket of the campaign. The Initiate Approvals field of the Execution screen reflects this default setting.

Depending on your business goals, you can export information from the finished campaign as an Audit Card for further processing, or implement changes from the campaign on the target configuration. You can also use the campaign as the basis for a recertification or differential campaign.

Differential Campaigns

A differential campaign is a recertification campaign that certifies new links added to the configuration that were not included in a previous campaign.

To implement a differential campaign, select the Differential option in the Campaign type field of the campaign creation wizard. The wizard presents options relevant to recertification campaigns, with the following special settings:

- No links from the previous campaign are included.
- The campaign includes only links that were added to the configuration after the previous campaign was created.

Depending on your business goals, you can export information from the finished campaign as an Audit Card for further processing, or implement changes from the campaign on the target configuration. You can also use the campaign as the basis for a recertification or differential campaign.

Define and Launch a Campaign

Use the campaign creation wizard to create a campaign, assign data files, and configure filters and other aspects of the campaign.

To define and launch a campaign:

1. Plan the [type, scope, and other features of the campaign](#) (see page 43) to meet your strategic business needs.
2. Verify that the data used in the campaign is updated and accurate, and create additional files needed for the campaign. These files can include:
 - Configuration files that clone or subset the model configuration of the universe
 - Audit cards that provide violation alerts or suggested links in the campaign
 - Member lists that map reviewers in the campaign
 - Customized email templates for the various messages CA RCM sends to campaign participants
3. Click Administration, Add Campaign from the main menu in the CA RCM portal.

The Campaign creation wizard appears.

4. Specify the following aspects of the campaign in the Campaign Type screen of the wizard:
 - The type of campaign to create.
 - The target universe
 - Other data sets of the campaign.
5. Specify the following aspects of the campaign in the [Basic information](#) (see page 48) screen of the wizard:
 - A name and short description of the campaign
 - Estimated duration of the campaign.
 - Whether to [include audit card violations](#) (see page 70) in the campaign.
6. [Define the entities and links to include in the campaign](#) (see page 71) in the [Filter screen](#) (see page 49) of the wizard.
7. Specify [how a certifying reviewer is assigned](#) (see page 63) to each link or entity under review. These settings appear in the Reviewers screen of the wizard. You can also allow reviewers to certify groups of entities, or require them to review and certify each entity individually.
8. Specify how suggested changes to the configuration are implemented. You can configure the following behaviors:
 - [Bypass Approval Processes](#) (see page 69)—you can select workflows that implement changes directly, without a secondary approval process.
 - [Rolling Approvals](#) (see page 69)—you can aggregate approval tasks in a second phase of the campaign, or implement approval/change processes on a rolling basis.
 - [Change target](#) (see page 50) - you can specify the configuration file in which changes are made.

These settings appear in the Execution screen of the wizard.

9. Specify the email templates to use for the various notification mails CA RCM sends to campaign participants. These settings appear in the Notifications screen of the wizard.
10. [Customize the table layout](#) (see page 56) in task tickets of the campaign.

11. Create and launch the campaign in the Summary screen. Launch options include:

- Manual launch—CA RCM generates the campaign, but does not send notifications to participating reviewers. The campaign owner launches the campaign from the top-level ticket of the campaign in their Inbox.
- Launch immediately—CA RCM generates the campaign and sends notifications to participating reviewers.
- Scheduled Launch—CA RCM generates the campaign, but only sends notifications to participating reviewers at the scheduled date and time.

Note: If you specify manual or scheduled launch, all data processing for the campaign is done immediately, based on the current contents of the configuration and other data files.

The campaign appears as a tree of tickets in your CA RCM inbox.

Basic Information Screen

Use this screen of the campaign creation wizard to specify a name, description, and other information for the campaign. The following fields are not self-explanatory:

Estimated Time

Defines the estimated duration of the campaign. After this time period, tickets related to the campaign are flagged as overdue, but the campaign continues.

Audit Card Alerts

Specifies whether to [include violations from an audit card](#) (see page 70) in the campaign. Options include the following:

None

Campaign does not include audit card information.

From this Audit Card

Campaign tickets flag links under review that appear in the specified audit card.

Generate an Audit Card for the campaign

During campaign initialization, an audit card is generated using the audit settings file specified for the target universe. Campaign tickets flag links under review that appear in this audit card.

Require comments when approving privileges with violations

If reviewers approve a link with audit card violations, they must add a comment that explains their decision to approve the link. This option is only available when you choose to apply an audit card to the campaign.

Filter Screen

Use this screen to limit the scope of entities and links that are included in a certification campaign. Depending on the type of campaign you create, the following areas appear in the screen:

Select Users/Roles/Resources

Defines which entities to include in the campaign based on attribute values.

Links

Specifies which direct, indirect, or dual links to include in the campaign.

Suggested Links

Specifies whether CA RCM suggests new links to certifiers in this campaign, based on links in the audit card, and which suggested links to include in the campaign.

When you specify an audit card for the campaign, the following fields appear:

Filter by Audit Card

Specifies how audit card data is used to filter the links that are included in the campaign. Options include:

No Audit Card Filter

Audit card violations are not used to filter the links in the campaign.

Include if in Audit Card

The campaign includes only links that are listed in the Audit Card. This campaign reviews links that violate business rules.

Include if not in Audit Card

The campaign includes only links that are not listed in the Audit Card.

For recertification and differential campaigns, the following fields appear:

Select States

Specifies which links are included in a recertification or differential campaigns, based on their last status in the previous campaign. Options include:

Pending

Includes links that were not reviewed in the previous campaign.

Approved

Includes links that were approved in the previous campaign.

Rejected

Includes links that were rejected in the previous campaign.

When you specify the Approved or Rejected options, specify one of the following options to specify how the decisions of the previous reviewers are handled:

Reset Approver's Selection

Omits the decisions of previous reviewers from the current campaign.

Keep Approver's Selections

Displays the decisions of previous reviewers in tickets of the current campaign. Reviewers can override the previous decision. This is the default setting.

Update Links

Specifies whether to add links from the configuration that were not in the previous campaign. Options include:

Add links that were not included in the source campaign

New and excluded links in the configuration are included in this campaign. An icon indicates these new links in certification tickets of the campaign.

Do not update

This campaign includes only links that were in the previous campaign.

Clone the Active Model Configuration for a Campaign

Often, you want to base a campaign on the model configuration, which reflects the most current picture of the universe. But campaigns must be based on a static, unchanging configuration - changes to the base configuration during the campaign can cause data inconsistencies. The active model configuration is updated only after the campaign concludes.

For these reasons, we strongly recommend that you *not* base a campaign directly on the active model configuration.

You can easily base a campaign on a copy of the active model configuration. By default, this option appears in the Configuration drop-down of the campaign creation wizard.

To clone the Active Model Configuration for a Campaign

1. Verify that the following system property is set to False:

campaign.settings.allowMasterAndModelCampaign

Specifies whether you can base a campaign on active master or model configurations of the target universe. Valid values are as follows:

True

Master and model configurations appear in the Configuration list of the Add Campaign screen.

Note: we strongly recommend that you *not* create campaigns based on the active master or model configurations.

False

Master and model configurations do not appear in the Configuration list of the Add Campaign screen. Instead, the option to base the campaign on a copy of the model configuration appears in the drop-down.

The campaign wizard offers the option to base the campaign on a clone of the model configuration.

2. Use the following system property to define how CA RCM names the clone of the model configuration.

campaign.settings.copyModelConfigurationNamePattern

Defines the format of the name that CA RCM applies when it copies the active model configuration for a campaign. This property defines a text string format, and can use the following placeholder parameters:

%configuration%

The name of the model configuration that is copied.

%campaignName%

The name of the campaign for which this copy was created. This is a required parameter that must appear in the property value.

%date%

The start date of the campaign.

Example: **the following formatting string includes two parameters:**

Copy of %configurationName% configuration for the %campaignName% campaign

For an original configuration named ActiveBaseConf and a campaign named InitialCertification, the resulting string is as follows:

Copy of ActiveBaseConf configuration for the InitialCertification campaign

When you create a campaign based on a clone of the model configuration, CA RCM names the new configuration file according to the specified pattern.

3. Create a campaign. In the Execution screen of the campaign creation wizard, select the In campaign configuration option.

CA RCM creates a clone of the model configuration, and bases the campaign on the clone. CA RCM implements any changes that result from the campaign on the clone configuration.

What You Can Do During a Campaign

During an active campaign, the administrator can perform the following actions:

- Review and certify any links directly assigned to them
- Reassign review tasks
- Attach a comment, file or link to a group of tasks
- Monitor campaign progress
- Send escalation emails to participating reviewers
- Suspend and restart the campaign
- [Save certification decisions](#) (see page 60) to an audit card
- Initiate the approval and implementation phase of the campaign

A certifying reviewer can perform the following actions:

- Review and certify any links directly assigned to them
- Reassign review tasks
- Attach a comment, file or link to a task or group of tasks

More information:

[Review and Certify Links](#) (see page 53)

[Reassign Links to Another Reviewer](#) (see page 54)

[Attach a Comment, File, or Link](#) (see page 55)

[Customize Ticket Tables](#) (see page 56)

[Monitor Campaign Progress](#) (see page 58)

[Define and Send Escalation Emails](#) (see page 58)

[Suspend and Restart a Certification Campaign](#) (see page 59)

[Initiate the Approval Phase of a Campaign](#) (see page 59)

[Certification Decisions](#) (see page 60)

Review and Certify Links

User privileges and role definitions are represented as a set of links between user, role, and resource entities. Your task as a certifier is to review the links in your ticket and approve or reject them.

To review and certify links

1. In your Inbox, click on a certification ticket.

The Certification Summary screen of the ticket appears. The upper General Information pane shows your progress in your review tasks. The Certify pane lists high-level groups of your certification tasks. The tasks are grouped by entity.

2. Click Certify beside a group to review the links in the group.

The My certification tasks screen appears. Each table shows links of the same type that relate to the entity named in the My certification tasks screen header. For example, the screen shows all roles and resources that are linked to one user, or all users and roles that link to one resource.

(Optional) If the campaign includes suggested links, these links are listed in separate Available Suggested entity tables.

3. (Optional) If the campaign includes violations information, the Alerts column appears. Click in the Alerts column beside a link to view business rules that the link violates.
4. (Optional) If the campaign includes usage information, the Usage column appears. An icon indicates the level of usage. Click the icon to view usage details.
5. Perform one of the following actions:
 - Click the Approve icon beside a link to indicate you accept the link.
 - Click the Reject icon beside a link to indicate you want to delete the link.
Note: If group selection is enabled for the campaign, click the checkbox in the Approve or Reject column header to approve or reject all links in a table.
 - Click the History icon to view the History of a link.
 - Click the Comment or Attachment icons to add a comment or attachment to a link.
6. (Optional) If the campaign includes suggested links, click Approve beside a link you want to add.

7. Click Save.

Your review decisions are saved. The Certification Summary screen indicates your progress.

Note: You can return to the same group of links several times to complete your review tasks.

Reassign Links to Another Reviewer

You can re-route to another reviewer links that CA RCM assigned to you or your subordinates. CA RCM places these reassigned links in the inbox of the new reviewer. CA RCM also updates the task tree in the inbox of the campaign owner to reflect the new distribution of tasks.

To reassign links to another reviewer

1. In your Inbox, click on a certification ticket.

Note: If you are a campaign administrator or a manager, click on a child in the campaign tree to reassign links for a subordinate reviewer.

The Certification Summary screen of the ticket appears. The upper General Information pane shows your progress in your review tasks. The Certify pane lists high-level groups of your certification tasks. The tasks are grouped by entity.

2. Click Certify beside a group.

The My certification tasks screen appears. Tables show similar types of links that are linked to one entity. The Default Assignee field below each column indicates the default target for reassigned links.

3. (Optional) Click the Default Assignee field to select another user as the default target for the table.

4. Click the Reassign icon beside links you want to send to another reviewer.

The Reassign column shows the target user for each link.

Note: If group selection is enabled for the campaign, click the checkbox in the Reassign column to reassign all links in a table.

5. (Optional) Click the target user of an individual link to reassign the link to another user.

6. Click Save.

The links are reassigned. The Certification Summary screen indicates your progress.

Attach a Comment, File, or Link

You can attach a text comment, data file, or a link to supporting information for a task or a group of tasks. This can be helpful when you reassign a link to another user for review.

In some campaigns, you may be required to provide a comment on your decisions - for example, you may be asked to justify approval for a link that violates business policy rules.

To attach a comment, file, or link

1. In your Inbox, click on a certification ticket.

Note: If you are a campaign administrator or a manager, click on a child in the campaign tree to work with links for a subordinate reviewer.

2. The Certification Summary screen appears. The Certify pane lists high-level groups of your certification tasks.
3. Do one of the following:

- Add a comment to a group:
 - a. Click the Comment icon beside a group.
 - b. The Comments pop-up appears.
 - c. Edit your comment.
 - d. Click OK.

The Comment icon shows the number of comments for the group.

- Add an attachment or link to a group:
 - a. Click the Attachment icon beside a group.
 - b. The Attachments pop-up appears.
 - c. Enter a description and browse to a file, or paste in URL.
 - d. Click Upload.
 - e. The file is added to the Attachments list.
 - f. Click Close.

The Attachment icon shows the number of attachments for the group.

4. Click Certify beside a group to review the links in the group.
The My certification tasks screen appears.

5. Do one of the following:

- Add a comment to a link:
 - a. Click the Comment icon beside a link.
 - b. The Comments pop-up appears.
 - c. Edit your comment.
 - d. Click OK.

The Comment icon shows the number of comments for the link.

- Add an attachment or link to a link:
 - a. Click the Attachment icon beside a link.
 - b. The Attachments pop-up appears.
 - c. Enter a description and browse to a file, or paste in URL.
 - d. Click Upload.
 - e. The file is added to the Attachments list.
 - f. Click Close.

The Attachment icon shows the number of attachments for the link.

Customize Ticket Tables

You can customize the default layout of tables in the tickets of a campaign. You can do this when you define the campaign in the campaign creation wizard, or from the root ticket of an active campaign that you administer.

When you change the layout of tables in a campaign that is already active, the changes are applied to new tickets and to tickets that have not been modified by users. If a user has customized the table layout of a ticket, their changes are preserved.

To customize ticket tables

1. Do one of the following:

- Create a campaign using the campaign creation wizard.

The Summary screen of the wizard appears.
- In your Inbox, click the root-level ticket of a certification campaign.

The Campaign View screen appears.

2. Click the Presentation bar.

The Presentation section of the screen opens. It contains three table headers:

- The Certification header shows the table layout of the Certification Summary screen for tickets related to the campaign.
- Depending on the type of campaign, User, Role, or Resource headers show the layout of each entity table in the My Certification tasks screen of the ticket.

3. Customize the tables:

- a. Click Customize on a table header you want to modify.

The Customize dialog appears.

- b. Use the arrow keys to add or remove column fields, and to order the columns.
- c. Click the lock icon to make a column mandatory. Mandatory columns appear in red. Users can move a mandatory column, but they cannot remove it.

Note: Mandatory fields defined for the universe appear in red. You cannot remove these fields from the table.

4. Click OK.

The table header reflects the changes you made.

5. Do one of the following:

- In the campaign creation wizard, review campaign settings and click Finish.

CA RCM creates the campaign and generates tickets with the layout you specified.

- In the root-level ticket of an active campaign, click Close.

Your Inbox appears. The layout you specified is applied to tickets of the campaign.

Monitor Campaign Progress

Campaign administrators monitor campaign progress from the root ticket of the campaign.

To monitor campaign progress

1. In your Inbox, click the root-level ticket of a certification campaign.
The Campaign View screen displays general information about the campaign and its current status.
2. Click View Campaign Progress.
A pop-up window shows the progress made by all reviewers in the campaign.

Define and Send Escalation Emails

Campaign administrators can send emails to remind reviewers to complete their tasks.

To define and send escalation emails.

1. In your Inbox, click the root-level ticket of a certification campaign.
The Campaign View screen displays general information about the campaign and its current status.
2. Click Escalation Emails
The Escalation Emails pop-up appears.
3. Configure the following information for each email you want to send:
 - Completion criteria
 - Email template
 - Email target
4. To add more emails, click the plus icon. To remove emails from the set, click the x icons.
5. (Optional) To save a set of email criteria:
 - a. Click Save.
 - b. The Save Escalation criteria pop-up appears.
 - c. Define a name for the email criteria, and click Save.
 - d. The email criteria are saved.

6. (Optional) To load a set of email criteria:
 - a. Click Load.
 - b. The Load Escalation criteria pop-up appears.
 - c. Select a set of email criteria, and click Load.
 - d. The email criteria are loaded.
7. Click Send Now.

Escalation emails are sent to reviewers with task completion that satisfies the criteria.

Suspend and Restart a Certification Campaign

Campaign administrators can start and stop the review phase of a campaign from the root ticket of the campaign.

To suspend and restart a certification campaign

1. In your Inbox, click the root-level ticket of a certification campaign.

The Campaign View screen displays general information about the campaign and its current status.
2. Click Stop Campaign.

The review phase of the campaign is suspended.
3. Click Re-Start Campaign.

The review phase of the campaign resumes.

Initiate the Approval Phase of a Campaign

Typically, you must stop the review phase of the campaign before you can start the approval and implementation phase.

Note: If you configured rolling approvals for the campaign, review and approval tasks are not separated into distinct phases.

To suspend and restart a certification campaign

1. In your Inbox, click the root-level ticket of a certification campaign.

The Campaign View screen displays general information about the campaign and its current status.
2. Click Stop Campaign.

The review phase of the campaign is suspended.

3. Click Start Approval Phase.

The approval and implementation phase of the campaign starts. CA RCM creates approval task tickets, and sends out email notifications to users who must approve changes to the user, role, and resource entities that they manage.

4. Go to your Inbox.

The certification campaign ticket tree is archived. A new approval task ticket tree appears.

Certification Decisions

You can save the decisions made by certifiers in a campaign to a data file. This data can form the basis for additional campaigns or analytical processes.

The data file is a variation of the standard audit card format. This audit card records the results of the initial certification review. The audit card does *not* filter those decisions based on the final approval phase of the campaign. All certification decisions are saved, even if resource owners or managers did not allow the requested changes.

Save Certification Decisions to an Audit Card

You can save the decisions certifiers make in a campaign to a data file. This data can form the basis for additional campaigns or analytical processes.

The data file is a variation of the standard audit card format. This audit card records the results of the initial certification review. The audit card does *not* filter those decisions based on the final approval phase of the campaign. All certification decisions are saved, even if resource owners or managers did not allow the requested changes.

To save certification decisions to an audit card

1. Click Administration, Campaign Administration from the main menu of the CA RCM portal.

The Campaign Administration screen appears.

2. Click Export Campaign Progress to Audit Card.

Note: To export from a campaign created in CA RCM release 3.2, click Export v3.2 Campaign to Audit Card.

The Export Campaign Progress to Audit Card screen appears.

3. Select an active campaign, enter the name of the audit card that contains saved data.

Note: If you specify an existing audit card, its data is overwritten.

4. Click Export.

An audit card is created that records the initial review phase of the campaign you specified. The audit card does *not* contain decisions from the final approval phase of the campaign.

Import Certification Decisions Into a Campaign

You can import the decisions certifiers made in a previous campaign into a new campaign.

To import certification decisions into a campaign

1. Create a campaign. In the Summary screen of the campaign creation wizard, specify the Disabled option in the Auto Start field.

CA RCM generates the campaign, but does not launch it.

2. Click Administration, Campaign Administration from the main menu of the CA RCM portal.

The Campaign Administration screen appears.

3. Click Import Certification Progress from Audit Card.

The Import Certification Progress from Audit Card screen appears.

4. Specify the inactive campaign and the audit card that contains saved data.

5. (Optional) Select the Delete Unchanged Tasks option to delete entities and links that do not match decisions in the audit card from the campaign.

The campaign contains only decisions that appear in the audit card.

Note: To use this option effectively, create a campaign that closely matches the scope and settings of the original campaign.

6. Click Import.

Review decisions from the audit card that reference entities and links in the campaign are copied to the campaign.

7. Go to your inbox to launch the campaign.

Certification and Approval Stages of a Campaign

Most certification campaigns involve two phases:

- **Certification**—Managers and resource owners review the links of the users, roles, and resources they administer. For example, a manager reviews the privileges of their staff members, or a role owner examines the resources included in the role.
- **Approval**—If a link is rejected during the review phase, or a new link is suggested, the manager of the linked resource must approve the proposed change. For example, if a manager rejects access to a certain resource for their worker, the owner of that resource must approve the change. Only rejected links or new links trigger approval tasks, because they change the base configuration.

By default, campaigns have distinct review and approval phases. Approval tasks are held until all certification tasks are complete. The campaign owner initiates the approval phase from the root ticket of the campaign. Approval tasks and notifications are consolidated, simplifying the work of resource owners.

You can configure the campaign so that approval tasks are initiated immediately when a reviewer submits a rejected link. The review and approval phases of the campaign overlap, and both review and approval tasks are active throughout most of the campaign. This campaign structure has several disadvantages, especially for campaigns with a large scope. Because approval tasks are not consolidated, resource owners and managers receive a separate email notification for each change they must approve. The approval phase is extended, and the volume of notifications and approval tasks can be distracting and unmanageable. Resource owners cannot assess the overall impact of changes resulting from the campaign.

How CA RCM Assigns Certifiers

CA RCM analyzes entity attributes to locate a manager or resource owner for each entity or link under review.

In *entity certification campaigns*, CA RCM can assign reviewers in the following ways:

- Search the RACI configuration of the universe for a user who is Accountable or Responsible for the entity.
Note: In user certification campaigns, CA RCM first queries the Configuration user manager field defined in the target universe to identify the manager of each user.
- Search a predefined member list in the server for a user related to the entity.
- Assign the task to a default reviewer defined for the campaign.
- Let users approve their own links. This option is only relevant to self attestation campaigns.

In *recertification and differential campaigns*, CA RCM can assign reviewers in the following ways:

- Search a predefined member list in the server for a user related to the entity.
- Use the same reviewer as the previous campaign.
- Assign the task to the manager of the previous reviewer, based on the Configuration user manager field specified for the target universe.
- Assign the task to a default reviewer defined for the campaign.

When you create a campaign you can define which of these techniques CA RCM uses to locate a certifier, and in what order they are used.

Example: Assign a Certifier

You can specify the following sequence to find certifiers for a campaign:

1. CA RCM first consults a member list. If a reviewer is found in the member list, the process stops.
2. If no reviewer is found in the member list, CA RCM then consults the RACI configuration. If a reviewer is found, the process stops.
3. If no reviewer is found in the RACI configuration, the certification task is assigned to a default reviewer.

Member Lists

A member list is a data set that contains user names and attributes. You use a member list to assign reviewers in a certification campaign.

A member list contains the following three fields:

Login

Defines a user account in CA RCM. This field has the same content and format as the LoginID field of a user or configuration file.

Category

Defines a user, role, or resource attribute. This field can have a different value for each record in the member list. To match entities in the campaign, specify attributes that exist in the configuration file on which the campaign is based.

Value

Defines the value of the attribute listed in the Category field.

To assign a reviewer for an entity under review, CA RCM scans the member list, comparing attribute values in the member list to the attribute values of the entity under review. CA RCM assigns review tasks for the entity to the user specified by the *first* record in the member list that matches an attribute value of the entity.

Note: A member list can only contain attributes for one entity type—user, role, or resource. However, one member list can contain attributes and values from several universes. Only the LoginID field must be uniformly defined in all universes that are used with the member list.

You perform the following member list administration functions through the CA RCM portal:

- Create a member list interactively.
- Import a data file to create a member list.
- Clone an existing member list to create a member list.
- Edit an existing member list interactively.

Example: Match Reviewers to Resource Attributes

The following member list associates users with various resource attribute values:

Login	Category	Value
DOMAIN\Hector_Torres	ResName3	Solaris
DOMAIN\Anna_ChIU	Location	Atlanta

Login	Category	Value
DOMAIN\Alex_Patrick	ResName3	WinNT
DOMAIN\Kim_Bell	Organization	Marketing Sun Server

This member list is used to assign reviewers in a resource certification campaign. The following resources are under review:

- The Domain_Users resource with ResName3 attribute equal to Solaris, and Location attribute equal to Atlanta. CA RCM uses the *first* matching record in the list, and assigns Hector Torres to review links for this resource.
- The Purchasing resource with Organization equal to Headquarters. No records in the member list match this entity. CA RCM cannot assign a reviewer based on the member list.

More information:

[Create a Member List](#) (see page 65)

[Clone a Member List](#) (see page 66)

[Create a Member List from a CSV File](#) (see page 67)

[Edit a Member List](#) (see page 68)

Create a Member List

You use a member list to assign reviewers for a campaign. There are several ways to create a member list. Use this procedure to interactively create a member list in the CA RCM portal.

To create a member list

1. From the CA RCM portal main menu, click Administration, Campaign Administration, Manage Member Lists.

The Member List main screen appears.

2. In the Add Member List area, define a new member list. the following field is not self-explanatory:

Campaign Type

Specifies the type of campaign that uses the member list. For example, a member list that contains role attributes works with a role certification campaign.

3. Clear the Use CSV file option.

4. Click Add.

The Edit member list screen appears.

5. Use the [Add, Edit, and Delete options](#) (see page 68) to compose the member list.

6. Click Save.

Changes are saved to the member list. The main Member lists administration screen appears. The new list appears in the table of member lists.

More information:

[Clone a Member List](#) (see page 66)

[Create a Member List from a CSV File](#) (see page 67)

[Edit a Member List](#) (see page 68)

Clone a Member List

You use a member list to assign reviewers in a campaign. There are several ways to create a member list. Use this procedure to create a member list based on a copy of an existing member list.

To clone a member list

1. From the CA RCM portal main menu, click Administration, Campaign Administration, Manage Member Lists.

The Member List main screen appears. A table lists the member lists in the CA RCM database.

2. Click the Copy icon of the member list that you want to copy.

The Copy member list screen appears.

3. Define a new name for the member list, and click OK.

Note: You cannot edit this name after the list is created.

A new member list appears in the table, with the name you defined. The list contains the same records as the base list.

4. Click the Edit icon of the new list.

The Edit member list screen appears.

5. Use the [Add, Edit, and Delete options](#) (see page 68) to modify the list.

6. Click Save.

Changes are saved to the member list. The main Member lists administration screen appears.

Create a Member List from a CSV File

You use a member list to assign reviewers for a campaign. There are several ways to create a member list. Use this procedure to create a member list based on an imported file of comma-separated values.

To create a member list from a CSV file

1. Prepare the data file. The first line of the CSV file must be the following header:

```
login,category,value
```

Note: Use only lower-case letters in this header line.

Each line of the file must contain three values, separated by commas. The following example shows a CSV file with two data records:

```
login,category,value
DOMAIN\Alex_Patrick,ResName3,WinNT
DOMAIN\Kim_Bell,Organization,Marketing Sun Server
```

2. From the CA RCM portal main menu, click Administration, Campaign Administration, Manage Member Lists.

The Member List main screen appears.

3. In the Add Member List area, define a new member list. the following field is not self-explanatory:

Campaign Type

Indicates the type of campaign that uses the member list. For example, a member list that contains role attributes works with a role certification campaign.

4. Click the Use CSV file option and browse to the CSV file you prepared.
5. Click Add.

CA RCM creates a member list file based on the CSV file. The member list is stored in the CA RCM database, and the new file appears in the list of member lists.

6. (Optional) Click Edit beside the new file to verify its contents.

Edit a Member List

You use a member list to assign reviewers in a campaign. Use this general procedure to edit member lists in the CA RCM portal.

To edit a member list

1. From the CA RCM portal main menu, click Administration, Campaign Administration, Manage Member Lists.

The Member List main screen appears. A table lists the member lists in the CA RCM database.

2. Click the Edit icon of the member list you want to edit.

The Edit member list screen appears.

3. Add a new record to the member list as follows:

- a. Select the configuration file on which this record is based. The drop-down lists available configurations.

- b. Click Add.

The Add entry pop-up appears.

- c. Select a user, attribute field, and value. Only values in the base configuration are available.

- d. Click OK.

The record is added to the member list, and appears in the table.

4. Edit a record in the member list as follows:

- a. Find the record in the table, and click the Edit icon of that record.

The Edit pop-up appears.

- b. Select a user, attribute field, and value. Only values in the base configuration of this record are available.

- c. Click OK.

The record is updated. New values for this record appear in the table.

5. To delete a record, find the record in the table, and click the Delete icon of that record.

The record is deleted from the member list.

6. Click Save.

Changes are saved to the member list. The main Member lists administration screen appears.

Immediately Invoke Approval Processes

You can create a campaign that initiates approval tasks immediately when each reviewer submits changes. The review and approval phases of the campaign overlap, and both review and approval tasks are active throughout most of the campaign.

To immediately invoke approval processes

1. In the Execution screen of the campaign creation wizard, find the Initiate Approvals field.
2. Select the As each certifier submits changes option for this field.
Approval-related tickets are activated and email notifications are sent immediately, as each certifier submits their changes.

Bypass Approval Processes for a Campaign

Typically, when changes result from a certification review, the owners of the entities involved must approve the changes. You can bypass this approval process in a campaign. CA RCM immediately implements all changes indicated during the initial certification review.

Important! Bypassing the approval process can have unexpected consequences. Only an experienced campaign manager should implement such a campaign, after consultation with the role engineer.

Because of the increased possibility of mistakenly overwriting configuration data, we recommend that you bypass approvals only in campaigns that are based on a copy or subset of configuration data. Do not use this option with campaigns that are based on the model configuration of the active universe or an original version of a configuration file.

To bypass approval processes for a campaign:

1. Verify that the value of the allowModifiedCampaignProcess system property is True.

allowModifiedCampaignProcess

Specifies whether campaign processes that bypass the approval task are available in the portal.

True

Makes review processes that bypass approval available during campaign creation.

False

Hides review processes that bypass approval. Only standard review processes - which include approval tasks - can be selected during campaign creation.

1. Copy a configuration file or create a partial file containing relevant data.
2. Create a campaign based on the configuration file you created.
3. In the Execution screen of the campaign creation wizard, drop-down fields let you specify the workflows used to remove rejected links.

In each Remove Link Process field, do *one* of the following:

- Select the Bypass Approval version of the process to skip approvals when that type of link is rejected. Rejected links are deleted without secondary approval.
- Select the regular version of the process to trigger approval tasks when that type of link is rejected.

Audit Card Violations in a Campaign

Audit cards list entities and links that are out-of-pattern or violate business process rules. This information can be useful to the certifier as they review entities and links during a campaign.

When you define a campaign, you can include information from an audit card in the base universe, or generate an audit card for the campaign. If a violation in the audit card refers to an entity under review, the entity is flagged in certification tickets of the campaign. Certifiers can click the item to view details of the violation.

How Campaigns Apply Pre-approved Violations

When a list of pre-approved violations has been defined for the universe, the list filters violations in all campaigns based on that universe.

In this case there are two audit cards: the audit card you specify as a source of violations when you create the campaign, and the audit card of pre-approved violations specified for the universe. Audit card violations are processed as follows for the campaign:

1. CA RCM identifies entities and links under review that appear in the audit card you specify when you create the campaign.
2. CA RCM filters this group of entities and links based on the audit card of pre-approved violations in the universe. If a violation from the campaign audit card appears in the pre-approved audit card, it is handled as configured for pre-approved violations in the universe: the alert is either ignored and not displayed, or it is dimmed.

More information:

[Pre-Approved Violations](#) (see page 191)

The Scope of a Campaign

When you create a campaign, you can define filtering criteria that limit the entities and links included in the campaign. The filters you define can dramatically alter the character of the campaign to support specific business needs. For example, you can restrict campaigns to subsets of users or resources using geographical location or other attributes. You can also combine multiple filters based on different criteria.

The [Filter screen](#) (see page 49) of the campaign creation wizard displays filter options relevant to the type of campaign you create.

Attribute Value Filters

You can filter the entities included in a campaign using entity attribute values.

You can also combine several attribute-based criteria.

Define these filters in the Filter screen of the campaign creation wizard.

Example: Roles Pending Approval

To certify roles that have been proposed, but not yet approved, define a role certification campaign with the following entity filter:

- Select roles with the Approval Status field equal to Pending Approval.

The campaign includes only roles that have not yet been approved.

Example: User Certification by Function and Location

To certify the privileges of sales staff in the Texas region, define a user certification campaign with the following entity filters:

- Select users with the Organization field equal to Sales.
- Select users with the Location field equal to Texas.
- Specify the All conditions option.

The campaign includes only users that match both conditions.

Link Type Filters

You can limit the scope of a campaign to certain types of links.

Entities in a configuration can be connected in three ways:

Direct Connection

Only an explicit, direct link connects two entities. There are no implicit links between them due to parent-child inheritance in the role hierarchy.

Indirect Connection

Two entities are connected only through a role, or through parent-child inheritance of links in the role hierarchy. There is no direct link between them.

Dual Connection

Two entities are linked both directly through an explicit link, and indirectly through the role hierarchy.

Define these filters in the Filter screen of the campaign creation wizard. In the Select Links area of the screen, specify the direct, indirect, and dual links you want to include in the campaign. To refine your selection, open the Direct, Indirect, and Dual fields to show a tree of links relevant to the type of campaign you are creating.

Audit Card Filters

If you associate an Audit Card with the campaign, you can use the audit card to filter which links are included in the campaign. The following options are available:

- No audit card filter—Audit card information is used to flag violations, but not to limit the scope of the campaign.
- Include only links that are in the audit card—Use this option to create a campaign that focuses on violations.
- Exclude links that are in the audit card—Reviewers do not waste time on links that are likely to be deleted.
- Suggest new links—Typically, reviewers certify the existing links between entities in a configuration. CA RCM can also suggest new links based on the audit card associated with the campaign. If a reviewer approves a suggested link, it is added to the configuration.

Previously Reviewed Links

When you create a recertification campaign, you can filter the review tasks carried forward to the new campaign based on their status in the old campaign. You can also specify how the decisions of the previous reviewers are handled.

Updated Links

Recertification campaigns are based on the review tasks of a previous campaign. When you create a recertification campaign, you can include links in the configuration that were not part of the previous campaign. These links can be new links that did not exist when the previous campaign was initiated, or existing links that were excluded from the previous campaign.

Usage Information from CA Enterprise Log Manager in a Campaign

When CA Enterprise Log Manager is deployed in your environment, CA RCM can display usage information drawn from CA Enterprise Log Manager in the tickets of a campaign. Reviewers can use this information when they certify links.

In campaign tickets, a colored icon indicates frequency of use. Reviewers can click the icon to open a window with more detailed usage information from CA Enterprise Log Manager. This window shows all usage data for the entity under review—CA Enterprise Log Manager does not filter usage data based on the CA RCM user hierarchy.

Note: The connection between CA RCM and CA Enterprise Log Manager is protected by a security certificate. Reviewers are prompted to install the security certificate on their computers the first time they view information from CA Enterprise Log Manager.

Data polling between CA RCM and CA Enterprise Log Manager is enabled and configured separately for each universe. When you enable polling of CA Enterprise Log Manager for a universe, all campaigns based on that universe display usage information.

More information:

[How to Use Data from CA Enterprise Log Manager](#) (see page 184)

DNA-based Approval Process

You can create an AuditCard in the CA RCM DNA module that reflects changes between two configurations (the pre-configuration and the post-configuration, similar to master and model configurations), and then submit the audit card for approval to the CA RCM Portal.

As a result, an approval ticket tree will be generated, similar to what happens when performing Self-Service tasks. However, as opposed the Self-service originated approval tickets (and Campaign originated approval tickets), DNA originated approval tickets are not automatically started, and you have to click Start Process in your Inbox.

How to Upgrade Campaigns from Earlier Versions

Certification campaigns that you created using release 12.5 SP1 or earlier of CA RCM are incompatible with the data schemas, system properties, and campaign management controls of this release. You can upgrade these campaigns and continue working with their data.

- For 4.x releases, and release 12.0, 12.5, and 12.5 SP1—use the Upgrade Legacy Campaigns screen in the CA RCM portal.
- For 3.x releases—save campaign data to an audit card, and apply this data to a new campaign.

Note: For more information, see the relevant upgrade section of the *Installation Guide* for this release.

Chapter 6: Using Dashboards

Dashboards use graphs and charts to provide a useful overview of role-based configurations and the results of statistical and rule-based analysis.

Click Dashboards on the CA RCM portal main menu to access these screens.

Some of these screens are also displayed by default on your home page.

Depending on the content of the dashboard, some or all of the following controls appear in the headers of the dashboard:

Settings

Opens a dialog you use to select data sets to include in the dashboard.

Customize

Opens a dialog you use to change how graphs and charts are displayed.

Draw Charts

Regenerates the graphs and charts of the dashboard.

Value, Percent

Specifies if graphs show absolute values or percentages.

This section contains the following topics:

[Configuration Dashboard](#) (see page 78)

[Audit Card Dashboard](#) (see page 79)

[Compliance Dashboard](#) (see page 79)

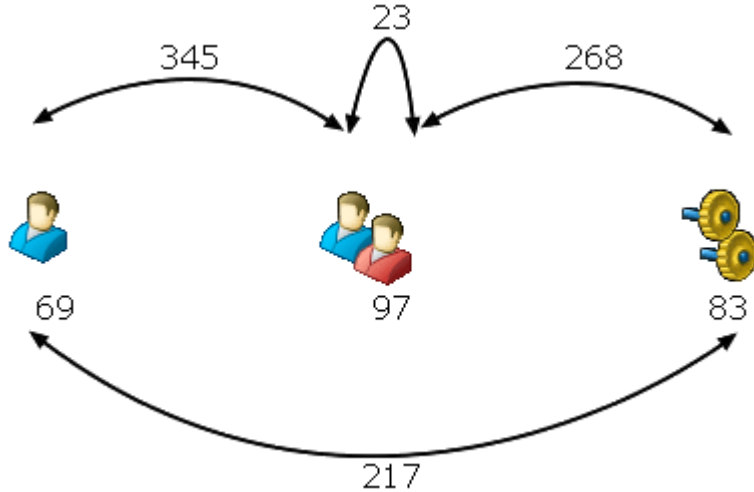
[Roles Coverage Dashboard](#) (see page 79)

[Certification Dashboard](#) (see page 80)

Configuration Dashboard

The configuration dashboard is a portal page that provides a graphical overview of the entities (users, resources, and roles) in a specified configuration, and the connections between them.

A graphic at the top of the page summarizes the users, resources, and roles in the specified configuration.



In the configuration shown, there are 69 users, 97 roles, and 83 resources. There are 345 user-role connections, and the role hierarchy contains 23 role-role connections.

A series of bar charts summarize the connections between users, roles, and resources. The following types of links are described:

Direct Connection

Only an explicit, direct link connects two entities. There are no implicit links between them due to parent-child inheritance in the role hierarchy.

Indirect Connection

Two entities are connected only through a role, or through parent-child inheritance of links in the role hierarchy. There is no direct link between them.

Dual Connection

Two entities are linked both directly through an explicit link, and indirectly through the role hierarchy.

Audit Card Dashboard

The audit card dashboard is a portal page that provides a graphical overview of the analytical alerts recorded in a specified audit card. By reviewing these violations, the Role Engineer can determine the current role configuration's goodness of fit and decide which direction to take to refine the configuration.

Note: The alert criteria reported in the audit card dashboard reflect the pattern analysis settings used to generate the selected audit card. For detailed information about these pattern analysis options, refer to the Sage DNA User Guide.

Compliance Dashboard

The compliance dashboard is a portal page that provides a graphical summary of possible violations of Business Policy Rules (BPRs).

Typically several audit cards affiliated with the same configuration file are selected for display on the dashboard. Use these graphs to compare the impact of different BPR rulesets, and to identify business policies that generate significant violations in the role configuration.

To populate the dashboard, scroll to the bottom of the page, select an audit card from the CA RCM database, and click **Add** to include the audit card's BPR alerts in the dashboard's graphs.

Note: The compliance dashboard accepts only audit cards that contain alerts related to Business Policy Rules (BPRs). Only BPR-related alerts are graphed; pattern-based alerts in the audit card are ignored.

Roles Coverage Dashboard

The roles coverage dashboard is a portal page that provides a graphical summary of the current role hierarchy, and how well the role hierarchy matches the underlying user, resource, and permission data.

The graphs of the dashboard show key measures in two related areas:

- **Coverage Indicators**—What portion of the actual user and resource privileges in the enterprise are included in the role hierarchy? How complete is the role hierarchy, and how well does it reflect actual permission patterns?
- **Quality Indicators**—How well-formed and efficient is the defined set of roles and business process rules? What portion of roles are sparsely populated with users, or in conflict with BPRs?

Certification Dashboard

The certification dashboard provides a graphical summary of the certification campaigns you participate in. It provides information about approved, rejected, reassigned, and pending review tasks for each campaign, and lists information about the performance of reviewers and approvers.

You can filter campaigns by type or by start date, and select individual campaigns to include in the dashboard.

Chapter 7: Running Self-Service Tasks

The CA RCM Portal's Self-Service feature provides local managers with the ability to do their own provisioning and/or provision their team-members on-the-fly, by adding or removing links between themselves/their team members and the corporation's roles and resources. The Self-Service tasks include the ability to create new roles or update existing one (only available to managers with appropriate permissions). Each task involves the functionality of one or more screens, which will be documented in this chapter.

In Adding Campaigns, we stated that managers do not update entity links during campaigns. They are limited to approving or rejecting the current links. At times, either following a campaign or following changes in corporate regulations or policies, it is necessary to update the actual links between the corporate users and the systems' roles and resources, or to generate new roles. This need is fulfilled by using the Self-Service tasks.

Note: The general functionality available in Self-Service task screens is already documented in [Using the CA RCM Portal Interface](#) (see page 15), and therefore, will not be documented in this chapter.

This chapter documents all the Self-Service tasks available via the CA RCM Portal. Managers will have access only to those features for which they have been provisioned. For the purpose of this manual, the Self-Service tasks are divided into two groups:

Provisioning Tasks

Includes all the tasks that manage a user's roles/resources:

- Manage my team's role assignments
- Manage my role assignments
- Manage my team's resource assignments
- Manage my resource assignments

Defining Roles Tasks

Includes the role definition tasks:

- Request a new role definition
- Request changes to a role definition

Note: If you find it necessary to run a Self-Service task that does not appear in your Self-Service menu, please report this to your system administrator.

The CA RCM Portal lets you add links to your favorite Self-Service tasks on the Home Page under My Business Processes.

This section contains the following topics:

- [General Self-Service Functions](#) (see page 83)
- [Manage My Team's Role Assignments](#) (see page 87)
- [Manage My Role Assignments](#) (see page 94)
- [Manage My Team's Resources](#) (see page 99)
- [Manage My Resources](#) (see page 106)
- [Defining a New Role](#) (see page 111)
- [Updating Role Definitions](#) (see page 117)
- [Introducing the Requests Table](#) (see page 118)

General Self-Service Functions

The Self-Service tasks functionality depends on the specific task that you undertake. Nevertheless, several functions are shared by several tasks.

This section describes two such functions:

- Test Compliance
- Suggest Entity

It is important to realize that you can use the Suggest Entity service to obtain a list of recommended entities, and yet the Test Compliance utility will find that the suggested links are in violation of system BPRs. The reason is that the Suggest Entity service is based on analytical pattern-based technology, while the Test Compliance utility examines the rules written by the system's administrators, rules that may or may not override the findings of the analytical pattern-based examination of the corporation's configuration files.

For example, the system may find that under certain conditions a specific application role is recommended for a group of users, and yet the Test Compliance utility will record this as a violation because the application is licensed and there are no free licenses available at this time.

More information:

[Test Compliance](#) (see page 83)

[Suggesting Entities](#) (see page 84)

Test Compliance

During a Self-Service provisioning task, you can test the compliance of your selections with the existing BPRs, security regulations and policies.

Note: For more information on violations stemming from non-compliance and other security issues see the *DNA User Guide*.


The Violations screen lists link entities that have a violation associated with them. If there are no violations, no records are listed.

The Violations screen groups entities by the rule or pattern condition that triggered the violation. All link entities that violate a specific rule or pattern are listed together. In addition to link information, the following field is displayed for each entity:

Score

The risk as defined for the specific BPR. The value is usually between 0 and 100.

To run the compliance testing

1. Click Test Compliance. The Violations screen opens in a separate browser window.
2. Click  in the upper right-hand corner to close the window.

Suggesting Entities

The CA RCM Portal takes advantage of the advanced pattern recognition technology provided by the CA RCM. This technology is utilized when you request that a CA RCM Portal's Self-Service task provide you with relevant suggestions, in various situations. For example, if you are seeking appropriate roles to add to your team's role assignments, using the Suggest Roles service will provide you with a weighted list of roles, where the weight is the result of pattern based analysis. For further information concerning the weights applied to the CA RCM pattern recognition technology see the *DNA User Guide*.

This service is provided for users, roles and resources as required.

The CA RCM Portal bases its suggestions on several available patterns. Not all patterns are available for all entities. The Suggest [Entities] service is available when you are requesting a suggestion for a recommended user, role or resource. The available options depend on the Self-Service task that is calling for the Suggest [Entities] service. The pre-defined patterns are:

Matching Rights

Used only for roles.

HR Pattern

Used for both roles and resources.

Privileges Pattern

Used for both roles and resources.

Matching Rule

Used only for roles.

Each one of these patterns is documented in detail in the *DNA User Guide*.

The pattern matching results appear in the columns of the relevant table:

- For provisioning tasks, the results appear in the Other Roles table.
- For role definition tasks, the results appear in the entity's designated table.

For the purposes of understanding what the CA RCM Portal is suggesting, the following table explains the logic behind these patterns:

Matching rights

The CA RCM looks at the current user's resources, which correlate (according to a given %) with the selected role's assigned resources, and suggests to enroll the current user in the selected role. The equivalent in the CA RCM DNA: "In/Out of Pattern": User matching.

HR Pattern

The CA RCM looks for users that are similar to the current user in terms of human resources attributes, and then looks at the common (limited by a pre-selected threshold) roles linked to those users, and suggests to add (some of the) common roles to the current user. The equivalent in the CA RCM DNA: "In/Out of Pattern": Propose new roles for users (by Human Resources).

Privileges Pattern

A generalized form of Matching Rights. The CA RCM looks at the current user's resources and compares them to the resources that other users have, and based on a pre-determined level of pattern matching, suggests to add (some of the) roles that the other users have, to the current user. The equivalent in the CA RCM DNA: "In/Out of Pattern": Propose new roles for users (by Privileges).

Matching Rule

The CA RCM looks at the role's rule, and finds the users that match the rule, but are not linked to the role, and suggests adding those users to the role. The equivalent in the CA RCM DNA: "In/Out of Pattern": Identify users matching rule based roles.

For more information see the *DNA User Guide, In/Out of Pattern Entities*.

When you request suggestions for more than one user, the table lists the number of users that match out of the number of selected users ([matching]/[selected]).

Click Suggest [Entity] to activate this service as part of a provisioning task. The table in which it is located changes and contains following columns:

Service	Added Columns
Suggest Roles	Four pattern columns plus a Details column.
Suggest Resources	<ul style="list-style-type: none"> ■ For Provisioning task screens: Two pattern columns plus a Details column. ■ For Role Definition task screens: The Enrolled column

Service	Added Columns
Suggest Users	The Enrolled column.

In a Provisioning task screen, click a highlighted link in the Details column and further information about the users and how they match the specific role/resource appears in a separate browser window.

Click  in the upper right-hand corner to close the window.

The Enrolled column, which appears in Role Definition task screens, provides the number of selected users/resources linked to this resource/user.

Manage My Team's Role Assignments

For the purposes of the CA RCM Portal, your team is essentially the users that you were assigned to manage. As a team manager, you may find it necessary to update role assignments because of corporate changes, personnel changes or following an audit process. The Manage My Team's Roles (MMT-Role) screen allows you to manage your team's roles, by generating a request to enroll your team in one or more roles, or by generating a request to enroll a specific user in one or more roles; or by severing the link between selected users and their current roles.

The role management utility allows you to manually select a specific target role, but it also provides you with a list of suggested roles and their pattern based behavior, thus giving you the information necessary to make an informed choice.

The screen is divided into four sections:

General

Provides descriptive information concerning the current action.

Users

Your team members. Select one or more users for the current action.

Currently Enrolled Roles

The current roles linked to the selected users.

Other Roles

Recommended roles for the selected users.

The Users and Other Roles sections present customizable tables.

As the MMT-Role screen allows many options and great flexibility, the task's procedures will be broken up by section:

- The fields in the General section
- The Users table options and functionality
- The Currently Enrolled Roles table options and functionality
- The Other Roles table options and functionality

To manage my team's role assignments, click Manage My Team's Role Assignments on the Self-Service menu. The Manage My Team's Roles screen opens.

More information:

[General Section \(MMT-Role Screen\)](#) (see page 88)

[Users Table \(MMT-Role Screen\)](#) (see page 89)

[Currently Enrolled Roles Table \(Manage My Roles Screen\)](#) (see page 90)

[Other Roles Table \(MMT-Role Screen\)](#) (see page 92)

General Section (MMT-Role Screen)

The General section of the Managing My Team's Roles screen contains the following fields:

Universe

Select the Universe you wish to work with. The users' table and the available roles depend on the universe.

Business Area

General information (descriptive). This information will appear in the Description field of the ensuing Self-Service Approval-Root ticket.

Business Process

General information (descriptive). This information will appear in the Description field of the ensuing Self-Service Approval-Root ticket.

Description

Provide a concise and meaningful description of the changes you intend to make to your team's roles.

Submit

Click to submit your request for changes.

To enter the data in the MMT-Role General section

1. Select a Universe from the drop-down list.
2. Enter the Business Area for the current action.
3. Enter the Business Process associated with the current action.
4. Enter a Description.

Users Table (MMT-Role Screen)

The Users table displays a list of the users in the selected Universe's configuration files. The members of your team are marked with a green dot next to their Person ID.

The Users table provides the following options:

Add

A column of check boxes, one per user. Select one or more. When you check multiple users, all the changes you make will be implemented for all selected users.

Person ID

Click any highlighted ID listed in this column to open the associated User's Card.

Get Roles

Provides a list of Currently Enrolled Roles for the selected users.

Customize

Allows you to determine the columns that will appear in the Users table.

Records per page

Select the number of records that will appear in the Users table.

Find Users

Opens the Select User filter screen to assist you in finding specific users.

Once you have selected the user(s) you want to manage at this time, you can click Get Roles to obtain a list of the roles currently associated with these users.

Note: If the actions you want to take do not involve the currently enrolled roles associated with the selected user, you can skip the Currently Enrolled Roles table and go to the Other Roles table.

To select users and obtain their roles

1. In the Users table, select one or more users. You can click Find Users to open the Select User screen.
2. Click Get Roles.

The roles linked to the selected user(s) appear in the Currently Enrolled Roles table. A list of roles that are not linked to the currently selected user(s) appears in the Other Roles table.

At this point you can choose to:

- Manage the current enrollment list
- Add additional roles to the selected users
- Do both.

If you do not want to manage the currently enrolled roles, skip to add roles to the selected users.

More information:

[Filter a Data Table](#) (see page 16)

Currently Enrolled Roles Table (Manage My Roles Screen)

This section allows you to manage the current roles enrollment for your selected users. The options available to you depend on how many users you have selected for the current action.

In the case of single-user selection, click Get Roles to view the list of roles linked to your selected user.

In this case, the only option available to you in this section is to select the Remove check box next to a role thereby severing the link between the user and the selected role.

If you choose more than one user, the Currently Enrolled Roles table will present an additional column: Enrollment.

In the case of multiple-user selection, you can:

- Select the Remove check box next to a role thereby severing the link between the users and the selected role.
- Select the Add check box next to a role to which only some of the selected users were enrolled, thereby linking all the chosen users to the selected role.

The Currently Enrolled Roles table provides the following options:

Add

A column of check boxes, one per role. Select one or more. The check boxes next to roles that are already linked to all selected users will be disabled.

Remove

A column of check boxes, one per role. Check one or more to remove the link between the selected users and the selected roles.

Enrollment

This column appears only when selecting multiple users. Numerically displays [# of users enrolled]/[total # of users selected], for example 2/3 means that two of the three selected users are enrolled to this role. This column also provides the value as a percentage, for example: 1/3 (33%).

Role Name

Click any highlighted role name listed in this column to open its Role Card.

Depending on the type of action you wish to take, you may find that after selecting the appropriate check boxes in this section you have completed the task. In this case you can ignore the Other Roles section and skip submit your requests by clicking Submit at the bottom of the Manage My Team's Roles screen.

To make selections in the Currently Enrolled Roles table

1. In the Currently Enrolled Roles table click the relevant check boxes in the Add and/or Remove columns.

At this point you can choose to:

- End the process at this point
- Add additional roles to the selected users.

If you do not want to add new roles, submit your requests.

Other Roles Table (MMT-Role Screen)

This section allows you to enroll your selected user(s) to additional roles of your choice. The actual enrollment will take place following a review process.

Note: When you click Get Roles in the Users section, a list of roles that are not linked to the currently selected user(s) appears in the Other Roles table.

In addition to managing the roles currently linked to the members of your team, you can also request that the system provide a list of recommended roles for your selected users. This list of roles will be displayed in the section Other Roles.

The Other Roles section provides the following options:

Add

A column of check boxes, one per role. Select one or more to link the selected users to additional roles.

Role Name

Click any highlighted role name listed in this column to open its Role Card.

Customize

Allows you to determine the columns that will appear in the Other Roles table.

Records per page

Select the number of records that will appear in the Other Roles table per page.

Find Roles

Opens the Select Role filter screen to assist you in locating specific roles.

Test Compliance

Checks whether the selections made in the Other Role table comply with existing policies and BPRs (Business Practice Rules).

Suggest Roles

Provides a list of possible roles based on the CA RCM pattern recognition technology.

This table presents you with several options:

- You can manually select one or more roles that you wish to link to the selected users.
- You can use the Find Roles filter option to find specific roles and then make a selection from the filtered list of roles.
- You can click Suggest Roles and use the information provided by this feature to link roles to the selected users.

After making your selection(s) you can test the compliance of your selections with the existing BPRs and policies.

You can decide to make the request despite any listed violations, or you can amend your selections.

Important! Remember that when selecting multiple users, all role-related choices apply equally to all the users. If at any point you alter the selected users, click [Get Roles](#) again.

To link roles to selected users

1. In the Manage My Team's Roles screen scroll down to the Other Roles table.
2. (Optional) Click Find Roles to access the Select Role filter screen.
3. (Optional) Click Suggest Roles to see the CA RCM Portal's recommendations.
4. Select one or more roles to link to the chosen users.
5. (Optional) Click Test Compliance to review your selections and check for possible violations.

The Violations screen opens in a separate browser window.

6. Click **X** to close the Violations window.
7. Click Submit.

The Requests screen opens.

More information:

[Filter a Data Table](#) (see page 16)

[Test Compliance](#) (see page 83)

[Suggesting Entities](#) (see page 84)

[Introducing the Requests Table](#) (see page 118)

Manage My Role Assignments

As a user, you may find it necessary to request an update to your roles because of corporate changes, personnel changes or following an audit process. The Manage My Role Assignment screen allows you to manage your roles, by generating a request to add new roles or by deleting existing roles.

The role management utility allows you to select a specific target role, but it also provides you with suggested roles and the information necessary to make an informed choice.

The screen is divided into three sections:

General

Provides descriptive information concerning the current action.

Currently Enrolled Roles

The current roles linked to the selected users.

Other Roles

A list of available roles.

The Other Roles section displays a customizable table.

As the Manage My Roles screen allows many options and great flexibility, the procedures will be broken up by section:

- The fields in the General section
- The Currently Enrolled Roles table options and functionality
- The Other Roles table options and functionality

To manage my role assignments, click Manage My Role Assignments on the Self-Service menu. The Manage My Roles screen appears.

More information:

[General Section \(Manage My Roles Screen\)](#) (see page 95)

[Currently Enrolled Roles Table \(Manage My Role Screen\)](#) (see page 96)

[Other Roles Table \(Manage My Role Screen\)](#) (see page 97)

General Section (Manage My Roles Screen)

The General section of the Managing My Roles screen contains the following fields:

Universe

Select the Universe you wish to work with. The users' table and the available roles depend on the universe.

Business Area

General information (descriptive). This information will appear in the Description field of the ensuing Self-Service Approval-Root ticket.

Business Process

General information (descriptive). This information will appear in the Description field of the ensuing Self-Service Approval-Root ticket.

Description

Provide a concise and meaningful description of the changes you intend to make to your roles.

Submit

Click to submit your request for changes.

To enter the data in the Manage My Roles General section

1. Select a Universe from the drop-down list.

The Currently Enrolled Roles table and the Other Roles table will show roles belonging to the selected Universe's configuration.

2. Enter the Business Area for the current action.
3. Enter the Business Process associated with the current action.
4. Enter a Description.

Note: If the actions you want to take do not involve your currently enrolled roles, you can skip the Currently Enrolled Roles table and skip to the Other Roles table.

If you do not wish to manage the currently enrolled roles, add roles to the selected users.

More information:

[Currently Enrolled Roles Table \(Manage My Role Screen\)](#) (see page 96)
[Other Roles Table \(Manage My Role Screen\)](#) (see page 97)

Currently Enrolled Roles Table (Manage My Role Screen)

This section lets you manage your current roles enrollment. When you selected the Universe, the CA RCM Portal provided the list of your current roles, within the universe's configuration.

The Currently Enrolled Roles table, for the Manage My Roles task, provides only one option: to select a Remove check box next to a role thereby severing the link between you and the selected role.

The Currently Enrolled Roles table provides the following functionality:

Add

A column of check boxes, one per role. This column is inactive in this screen.

Remove

A column of check boxes, one per user. Check one or more to remove the link between the selected users and the selected roles.

Role Name

Click any highlighted role name listed in this column to open its Role Card.

Depending on the type of action you wish to take, you may find that after selecting the appropriate check boxes in this section you have completed the task. In this case you can ignore the instructions in the Other Roles and submit your requests by clicking Submit at the bottom of the Manage My Roles screen.

To make selections in the Currently Enrolled Roles table, in the Currently Enrolled Roles table click the relevant check boxes in the Remove column.

At this point you can choose to:

- End the process at this point
- Add roles.

If you do not want to add new roles, submit your requests.

More information:

[Other Roles Table \(Manage My Role Screen\)](#) (see page 97)

Other Roles Table (Manage My Role Screen)

This section allows you to enroll in additional roles of your choice. The actual enrollment will take place following a review process.

In addition to managing the roles that you are currently linked to, you can also request that the system provide you with a list of recommended roles for yourself. This list of roles will be displayed in the section Other Roles.

The Other Roles section provides the following options:

Add

A column of check boxes, one per role. Select one or more.

Role Name

Click any highlighted role name listed in this column to open its Role Card.

Customize

Allows you to determine the columns that will appear in the Other Roles table.

Records per page

Select the number of records that will appear in the Other Roles table per page.

Find Roles

Opens the Select Role filter screen to assist you in locating specific roles.

Test Compliance

Checks whether the selections made in the Other Roles table comply with existing policies and BPRs (Business Practice Rules).

Suggest Roles

Provides a list of possible roles based on the CA RCM pattern recognition technology.

This table presents you with several options:

- You can manually select one or more roles to which you wish to enroll.
- You can use the Find Roles filter option to find specific roles and then make a selection from the filtered list of roles.
- You can click Suggest Roles and use the information provided by this feature to find roles to which you should enroll.

After making your selection(s) you can test the compliance of your selections with the existing BPRs and policies.

You can decide to make the request despite any violations, or you can amend your selections.

To link to additional roles

1. In the Manage My Roles screen scroll down to the Other Roles table.
2. (Optional) Click Find Roles to access the Select Role filter screen.
3. (Optional) Click Suggest Roles to see the CA RCM Portal's recommendations.
4. Select one or more roles to link to the chosen users.
5. (Optional) Click Test Compliance to review your selections and check for possible violations.

The Violations screen opens in a separate browser window. Click **X** to close the Violations window.

6. Click Submit.

The Requests screen opens.

More information:

[Test Compliance](#) (see page 83)

[Suggesting Entities](#) (see page 84)

[Introducing the Requests Table](#) (see page 118)

Manage My Team's Resources

For the purposes of the CA RCM Portal, your team is essentially the users that you were assigned to manage. As a team manager, you may find it necessary to update resources because of corporate changes, resource updates or following an audit process. The Manage My Team's Resources (MMT-Resources) allows you to manage your team's resources:

- By generating a request to add new resources, for either a specific user or a for a group of users
- By severing the link between selected users and their current resources

The resource management utility allows you to manually select a specific target resource, but it also provides you with a list of suggested resources and their pattern based behavior, thus giving you the information necessary to make an informed choice.

The screen is divided into four sections:

General

Provides descriptive information concerning the current action.

Users

Your team members. Select one or more users for the current action.

Currently Enrolled Roles

The current resources linked to the selected users.

Other Roles

Recommended resources for the selected users.

The Users and Other Resources sections present customizable tables.

As the MMT-Resources screen allows many options and great flexibility, the task's procedures will be broken up by section:

- The fields in the General section
- The Users table options and functionality
- The Currently Enrolled Resources table options and functionality
- The Other Resources table options and functionality

To manage my team's resource assignments, click Mange My Team's Resource Assignments on the Self-Service menu. The Manage My Team's Resources screen opens.

More information:

[General Section \(MMT-Resources Screen\)](#) (see page 100)

[Users Table \(MMT-Resources Screen\)](#) (see page 101)

[Currently Enrolled Resources Table \(Manage My Roles Screen\)](#) (see page 102)

[Other Resources Table \(MMT-Resources Screen\)](#) (see page 104)

General Section (MMT-Resources Screen)

The General section of the Managing My Team's Resources screen contains the following fields:

Universe

Select the Universe you wish to work with. The users' table and the available resources depend on the universe.

Business Area

General information (descriptive). This information will appear in the Description field of the ensuing Self-Service Approval-Root ticket.

Business Process

General information (descriptive). This information will appear in the Description field of the ensuing Self-Service Approval-Root ticket.

Description

Provide a concise and meaningful description of the changes you intend to make to your team's resources.

Submit

Click to submit your request for changes.

To enter the data in the MMT-Resource General section

1. Select a Universe from the drop-down list.
2. Enter the Business Area for the current action.
3. Enter the Business Process associated with the current action.
4. Enter a Description.

Users Table (MMT-Resources Screen)

The Users table displays a list of the users in the selected Universe's configuration files. The members of your team are marked with a green dot next to their Name.

The Users table provides the following options:

Add

A column of check boxes, one per user. Select one or more. When you select multiple users, all the changes you make will be implemented for all selected users.

Person ID

Click any highlighted ID listed in this column to open the associated User's Card.

Get Resources

Provides a table of Currently Enrolled Resources for the selected users.

Customize

Allows you to determine the columns that will appear in the Users table.

Records per page

Select the number of records that will appear in the Users table.

Find Users

Opens the Select User filter screen to assist you in finding specific users.

Once you have selected the users you want to manage at this time, you can click Get Resources to obtain a list of the resources currently associated with these users.

Note: If the actions you want to take do not involve the currently enrolled resources associated with the selected user, you can skip the Currently Enrolled Resources table and go to the Other Resources table.

To select users from the MMT-Resources Users table and obtain their roles

1. In the Users table, select one or more users. You can click Find Users to open the Select User screen.
2. Click Get Resources.

The resources linked to the selected user(s) appear in the Currently Enrolled Resources table. A list of resources that are not linked to the currently selected user(s) appears in the Other Resources table.

At this point you can choose to:

- Manage the current enrollment list
- Add additional resources to the selected users
- Do both.

If you do not want to manage the currently enrolled resources, add resources to the selected users.

More information:

[Filter a Data Table](#) (see page 16)

[Currently Enrolled Resources Table \(Manage My Roles Screen\)](#) (see page 102)

[Other Resources Table \(MMT-Resources Screen\)](#) (see page 104)

Currently Enrolled Resources Table (Manage My Roles Screen)

This section allows you to manage the current resources enrollment for your selected users. The options available to you depend on how many users you have selected for the current action.

In the case of single-user selection, click Get Resources, and you will receive the list of resources linked to your chosen user.

In this case, the only option available to you in this section is to click the Remove check box next to a resource thereby severing the link between the user and the selected resource.

If you choose more than one user, the Currently Enrolled Resources table will present an additional column: Enrollment.

In the case of multiple-user selection, you can:

- Click the Remove check box next to a resource thereby severing the link between the users and the selected resource.
- Click the Add check box next to a resource to which only some of the selected users were enrolled, thereby linking all the chosen users to the selected resource.

The Currently Enrolled Resources table provides the following options:

Add

A column of check boxes, one per resource. Select one or more. The check boxes next to resources that are already linked to all selected users will be disabled.

Remove

A column of check boxes, one per resource. Check one or more to remove the link between the selected users and the selected resources.

Enrollment

This column appears only when selecting multiple users. Shows numerically [# of users enrolled]/[total # of users selected], for example 2/3 means that two of the three selected users are enrolled to this resource. This column also provides the value as a percentage. For example: 1/3 (33%).

Resource Name

Click any highlighted resource name listed in this column to open its Resource Card.

Depending on the type of action you wish to take, you may find that after selecting the appropriate check boxes in this section you have completed the task. In this case you can ignore the Other Resources and submit your requests by clicking Submit at the bottom of the Manage My Team's Resources screen.

To make selections in the Currently Enrolled Resources table, in the Currently Enrolled Resources table click the relevant check boxes in the Add and/or Remove columns.

At this point you can choose to:

- End the process at this point
- Add additional resources to the selected users.

If you do not want to add new resources, submit your requests.

Other Resources Table (MMT-Resources Screen)

This section allows you to enroll your selected user(s) to additional resources of your choice. The actual enrollment will take place following a review process.

Note: When you click Get Resources in the Users section, a list of resources that are not linked to the currently selected user(s) appears in the Other Resources table

In addition to managing the resources currently linked to the members of your team, you can also request that the system provide a list of recommended resources for your selected users. This list of resources will be displayed in the section Other Resources.

The Other Resources section provides the following options:

Add

A column of check boxes, one per role. Select one or more to link the selected users to additional resources.

Res Name 1

Click any highlighted resource name listed in this column to open its Resource Card.

Customize

Allows you to determine the columns that will appear in the Other Resources table.

Records per page

Select the number of records that will appear in the Other Resources table.

Find Resources

Opens the Select Resources filter screen to assist you in locating specific resources.

Test Compliance

Checks whether the selections made in the Other Resources table comply with existing policies and BPRs (Business Process Rules).

Suggest Resources

Provides a list of possible resources based on the CA RCM pattern recognition technology.

This table presents you with several options:

- You can manually select one or more resources that you wish to link to the selected users.
- You can use the Find Resources filter option to find specific roles and then make a selection from the filtered list of resources.
- You can click Suggest Resources and use the information provided by this feature to link resources to the selected users.

After making your selection(s) you can test the compliance of your selections with the existing BPRs and policies.

You can decide to make the request despite any listed violations, or you can amend your selections.

Important! Remember that when selecting multiple users, all resource-related choices apply equally to all the users. If at any point you alter the selected users, click [Get Resources](#) again.

To link resources to selected users

1. In the Manage My Team's Resources screen scroll down to the Other Resources table.
2. (Optional) Click Find Resources to access the Select Resource filter screen.
3. (Optional) Click Suggest Resources to see the CA RCM Portal's recommendations.
4. Select one or more resources to link to the chosen users.
5. (Optional) Click Test Compliance to review your selections and check for possible violations.

The Violations screen opens in a separate browser window. Click **X** to close the Violations window.

6. Click Submit.

The Requests screen opens.

More information:

[Filter a Data Table](#) (see page 16)

[Suggesting Entities](#) (see page 84)

[Test Compliance](#) (see page 83)

Manage My Resources

As a user, you may find it necessary to request an update to your resources because of corporate changes, resource changes or following an audit process. The Manage My Resources screen allows you to manage your resources, by generating a request to add new resources or by deleting existing resources.

The screen is divided into three sections:

General

Provides descriptive information concerning the current action.

Currently Enrolled Resources

The current resources linked to the selected users.

Other Resources

A list of available resources.

The Other Resources section displays a customizable table.

As the Manage My Resources screen allows many options and great flexibility, the procedures will be broken up by section:

- The fields in the General section
- The Currently Enrolled Resources table options and functionality
- The Other Resources table options and functionality

To manage my resources, click Manage My Resource Assignments on the Self-Service menu. The Manage My Resources screen appears.

More information:

[General Section \(Manage My Resources Screen\)](#) (see page 107)

[Currently Enrolled Resources Table \(Manage My Resources Screen\)](#) (see page 108)

[Other Resources Table \(Manage My Resources Screen\)](#) (see page 108)

General Section (Manage My Resources Screen)

The General section of the Managing My Resources screen contains the following fields:

Universe

Select the Universe you wish to work with. The users' table and the available resources depend on the universe.

Business Area

General information (descriptive). This information will appear in the Description field of the ensuing Self-Service Approval-Root ticket.

Business Process

General information (descriptive). This information will appear in the Description field of the ensuing Self-Service Approval-Root ticket.

Description

Provide a concise and meaningful description of the changes you intend to make to your resources.

Submit

Click to submit your request for changes.

To enter the data in the Manage My Resources General section

1. Select a Universe from the drop-down list.

The Currently Enrolled Resources table and the Other Resources table shows resources belonging to the selected Universe's configuration.

2. Enter the Business Area for the current action.
3. Enter the Business Process associated with the current action.
4. Enter a Description.

Note: If the actions you want to take do not involve your currently enrolled resources, you can skip the Currently Enrolled Resources table and skip to the Other Roles table.

If you do not want to manage the currently enrolled resources, add resources to the selected users.

Currently Enrolled Resources Table (Manage My Resources Screen)

This section lets you manage your current resource enrollment. When you originally selected the Universe, the CA RCM Portal provided the list of your current resources, within the universe's configuration.

In this case, the only option available to you in this section is to click the Remove check box next to a resource thereby severing the link between you and the selected resource.

The Currently Enrolled Resources table provides the following options:

Remove

A column of check boxes, one per user. Check one or more to remove the link between the selected users and the selected resources.

Res Name 1

Click any highlighted resource name listed in this column to open its Resource Card.

Depending on the type of action you wish to take, you may find that after selecting the appropriate check boxes in this section you have completed the task. In this case you can ignore the Other Resources and submit your requests by clicking Submit at the bottom of the Manage My Resources screen.

To make selections in the Currently Enrolled Resources table, in the Currently Enrolled Resources table click the relevant check boxes in the Remove column.

At this point you can choose to:

- End the process at this point
- Add resources

If you do not want to add new resources, submit your requests.

Other Resources Table (Manage My Resources Screen)

This section allows you to enroll in additional resources of your choice. The actual enrollment will take place following a review process.

In addition to managing the resources that you are currently linked to, you can also request that the system provide you with a list of recommended resources for yourself. This list of resources will be displayed in the section Other Resources.

The Other Resources section provides the following options:

Add

A column of check boxes, one per resource. Select one or more.

Res Name 1

Click any highlighted resource name listed in this column to open its Resource Card.

Customize

Allows you to determine the columns that will appear in the Other Resources table.

Records per page

Select the number of records that will appear in the Other Resources table.

Find Resources

Opens the Select Resource filter screen to assist you in locating specific resources.

Test Compliance

Checks whether the selections made in the Other Resource table comply with existing policies and BPRs (Business Practice Rules).

Suggest Resources

Provides a list of possible resources based on the CA RCM pattern recognition technology.

This table presents you with several options:


- You can manually select one or more resources to which you wish to enroll.
- You can use the Find Resources filter option to find specific resources and then make a selection from the filtered list of resources.
- You can click Suggest Resources and use the information provided by this feature to find resources to which you should enroll.

After making your selection(s) you can test the compliance of your selections with the existing BPRs and policies.

You can decide to make the request despite any violations, or you can amend your selections.

To link to additional resources

1. In the Manage My Resources screen scroll down to the Other Resources table.
2. (Optional) Click Find Resources to access the Select Resource filter screen.
3. (Optional) Click Suggest Resources to see the CA RCM Portal's recommendations.
4. Select one or more resources to link to the chosen users.
5. (Optional) Click Test Compliance to review your selections and check for possible violations.

The Violations screen opens in a separate browser window. Click  to close the Violations window.

6. Click Submit.

The Requests screen opens.

More information:

[Filter a Data Table](#) (see page 16)

[Test Compliance](#) (see page 83)

[Suggesting Entities](#) (see page 84)

[Introducing the Requests Table](#) (see page 118)

Defining a New Role

The term “roles” as used by the CA RCM is flexible and versatile, allowing it on one hand to answer the need to define roles that comprise a class of access privileges and on the other hand answer the need to define roles that represent organizational structures within a business context. For example, a role can represent access to a specific type of software, or a role can represent a hierarchical business structure component such as Manager Privileges.

Using the CA RCM to build and maintain a corporate role model requires the flexibility to approach this issue from two points of view. The first is by planning the corporate roles and defining them accordingly, based on the organizational structure and other, human resources related, attributes. The second is by mining existing corporate security and privileges information and structuring roles in a “bottom-up” approach, to match the enterprise privileges requirements.

The CA RCM Portal allows you to define new roles on-the-fly. When the need arises to define a new role, whether following an audit or in the course of an enterprise's life cycle, you can do so directly and quickly. The procedure comprises two screens:

- Request New Role Definition
- Definitions For Role Name [New Role Name]

More information:

[Request New Role Definition Screen](#) (see page 111)

[Definitions for Role Name \[New Role Name\]](#) (see page 115)

Request New Role Definition Screen

The first step in defining a new role is to define its characteristics and general definitions. For example, for a new role called Security Officer, you have to provide the role name, corporate definitions and rules that will govern this role.

The Request New Role Definition screen is divided into two sections:

- Task definitions
- Role definitions

The Task Definitions area includes the following fields:

Universe

Select the Universe you wish to work with. The new role will be associated with this universe's configuration. The users' table and the available resources provided in the Definitions for Role Name [New Role] screen depend on the universe.

Business Area

General information (descriptive). This information appears in the Description field of the ensuing Self-Service Approval-Root ticket.

Business Process

General information (descriptive). This information appears in the Description field of the ensuing Self-Service Approval-Root ticket.

Request Description

Provide a concise and meaningful description of the new role and its purpose.

The role definitions area includes the following fields:

Role Name

The name of the new role (concise and descriptive).

Description

Describe the new role.

Owner

Provide the owner ID. You can use the Find function to open the Find User filter.

Type

Provide the role type (use autocomplete).

Organization

Provide the name of the main organization (use autocomplete).

Organization 2

Provide the name of the secondary organization (use autocomplete).

Organization 3

Provide the name of the tertiary organization (use autocomplete).

Rule

(Optional) Provide a rule for the new Role. You can use the Add Rule function to construct a rule.

To define a new role, first screen

1. Click Request a New Role Definition on the Self-Service menu.
The Request New Role Definition screen opens.
2. Select a Universe from the drop-down list.
The newly defined role is associated with the configuration belonging to this universe. The users and resources to be linked with this role is taken from this universe's configuration.
3. Enter the Business Area for the current action.
4. Enter the Business Process associated with the current action.
5. Enter the Request Description.
6. Enter the Role Name.
7. Enter the Description of the new role.
8. Enter the Owner's ID. (Optional) Click Find to access the Find User filter screen.
9. Select a user from the User list generated by your filter. Click OK.
10. Enter a Type (use autocomplete).
11. Enter an Organization name (use autocomplete).
12. Enter an Organization 2 name (use autocomplete).
13. Enter an Organization 3 name (use autocomplete).
14. Create a Rule. Click Add Rule for assistance in constructing a rule.
15. Click Next. The Definitions for Role Name [Role Name] screen opens.

More information:

[Filter a Data Table](#) (see page 16)

[Constructing a Rule](#) (see page 114)

[Definitions for Role Name \[New Role Name\]](#) (see page 115)

Constructing a Rule

The CA RCM Portal provides you with the Add Rule utility to assist you in constructing a rule for the new role you are requesting.

This screen has the following text boxes and functions:

Field

Use autocomplete to select a field name.

Value

Enter a value or use autocomplete to provide an appropriate value.

Add

Lets you add another constraint to the rule.

Remove

Removes the last added constraint.

Cancel

Cancels the rule construction.

Note: Adding a rule is optional. Not every Role has to be rule-based.

To construct a rule

1. Click Add Rule in the Request New Role Definition screen.
The Rule Construction screen opens.
2. Enter a Field name.
3. Enter a Value.
4. (Optional) Click Add to add additional constraints.
5. Repeat step 2 to step 4 as necessary.
6. Click OK.

The constructed rule appears in the Rule text box in the Request New Role Definition screen.

Definitions for Role Name [New Role Name]

Now that you have requested a new role, you can start assigning users and resources to the newly constructed role. Roles can be linked to users, resources and to other roles in a hierarchal relationship as either a parent role or a child role. The Definitions for Role Name [New Role Name] screen provides you with a fast and easy way to select which links your new role will have.

When you have completed your selections, you can test those selections for violations. If you are satisfied with the results, click Submit, located below the entity tables, to generate a request for a new role definition. The request can be checked by you, and if you have no corrections to make, click Submit below the request table, and generate the approval process tickets necessary to confirm the role definitions that you have created.

Note: The users marked with a green dot next to their name in the Users table, are users that are accountable to you (RACI).

This screen is divided into three sections:

- Resources
- Users
- Role Hierarchy - which can expand into two sections:
 - Parent Roles
 - Children Roles

Role hierarchy evolves from role trees that are present in many corporate systems. For example, an Identity Manager application can have two levels of roles: Provisioning Role and Provisioning Policy. Users are always linked to a Provisioning Role that is linked to a specific Provisioning Policy. This hierarchal structure is maintained during import/export. When generating a new role, it is important to know whether there are system rules that demand specific hierarchal connections between roles.

Each section contains a customizable entity table listing all the relevant entities. To assist you in your selection the following functions are available:

Find Entities

Provides a filter screen.

Suggest Entities

Provides suggested users for selected resources or suggested resources for selected users. This service is not available for the Role Hierarchy tables.

Highlighted Column

In each customizable table there is one pre-defined column that is highlighted. Click the name of the entity to access its data card.

Customize

Provides the option to select the fields that will appear in the specified table.

Records per page

Select the number of records per page.

Test Compliance

Tests the selections you made for violations.

If you select to apply the Suggest Entities service to both users and resources, you see data on the enrollment of the users and resources.

To assign users, resources and role hierarchy to the new role

1. Select users, resource and/or role hierarchy entities. Utilize the Find Entity filter and the Suggest Entity utility when necessary.
2. Click Test Compliance to check your selections for violations.
3. Click Submit to submit the new role definition request.

The Requests screen opens. The Requests screen provides both the new role's attributes and links.

4. Click Back to amend the data.
5. Click Submit to forward the request to generate a new role.

More information:

[Request New Role Definition Screen](#) (see page 111)

[Filter a Data Table](#) (see page 16)

[Suggesting Entities](#) (see page 84)

[Test Compliance](#) (see page 83)

[Introducing the Requests Table](#) (see page 118)

Updating Role Definitions

The CA RCM Portal allows you to update role attributes and links on-the-fly.

When the need arises to update an existing role, whether following an audit or in the course of an enterprise's roles and privileges maintenance life cycle, you can do so directly and quickly. The procedure includes finding the role within a specific universe and then following the procedure described in *Defining a New Role*, though in this case, the fields have already been filled, the attributes defined and the links listed and your goal is to edit these selections to match your corporation's new needs.

In the Request Role Update screen, you are required to select a Universe. Selecting the Universe opens the Select Role screen.

This is a search screen with built-in filters and a RACI based advanced search feature.

Note: The universe's model configuration is listed in the upper right-hand corner of the Select Role screen.

Once you have successfully constructed a search pattern, a list of roles is displayed in the Role table.

To update an existing role

1. Click Request Changes to a Role Definition on the Self-Service menu.
The Request Role Update screen opens.
Select a Universe from the drop-down list.
2. Click OK.
3. The Select Role screen opens.
4. Filter the data table to create a search pattern.
5. (Optional) You can use the RACI based Advanced Search feature to include additional constraints on the search.
6. Click Search.
A list of roles is displayed in the customizable Role table.
7. Select the Add check box for the role you want to update.
8. Click OK.
The Request Role Update screen opens.

More information:

[Defining a New Role](#) (see page 111)

[Filter a Data Table](#) (see page 16)

[Request New Role Definition Screen](#) (see page 111)

[Definitions for Role Name \[New Role Name\]](#) (see page 115)

Introducing the Requests Table

Each Self-Service task requires you to submit a request to perform the changes generated via the task's screens. When you have finished your selections in the selected Self-Service screen and have clicked Submit, the Requests screen appears. This screen summarizes the requests you have made while performing the Self-Service task.

Depending on the Self-Service task, the Request screen may contain additional information. For example, when generating a new role request, the Requests screen will also include the Attribute data for the new role.

The columns in the Links table provided in this screen depend on the type of Self-Service request you have just processed. Highlighted data gives you access to the relevant entity cards and further information. This information always includes the following two columns:

Request

Presents the nature of the Self-Service request. The options are Remove or Add.

Violations

Presents the number of violations associated with the specific request. Click on the number to view further details.

At this point the CA RCM Portal supplies you with two functions:

Back

To return to the previous screen and edit your selections.

Submit

Sends your request to the CA RCM for processing. The Generating Tickets progress bar appears.

In the case of provisioning type Self-Service tasks, if no errors are found, a Self-Service ticket tree will be generated and placed in your inbox. For each request listed in the Request table, one branch appears in the Self-Service ticket tree.

When generating a new role or updating an existing one, other tickets will be generated as needed.

1. (Optional) Click Back to return to the previous screen to amend your selections.
2. Click Submit to generate the Self-Service request tickets. The Requests Sent screen appears.

The Requests Sent screen lists the new ticket ID (the ID of the ticket owner's root ticket). You can view the new ticket tree in the Inbox.

More information:

[Running Self-Service Tasks](#) (see page 81)

[Role Definition Tickets](#) (see page 121)

Chapter 8: Role Definition Tickets

This chapter is designed for managers who can run Self-Service based Approval Processes and for entity managers who may receive Approver tickets as part of the Self-Service approval process.

Self-Service requests can be divided into two basic types:

Provisioning tasks

- Manage my team's role assignments
- Manage my role assignments
- Manage my team's resource assignments
- Manage my resource assignments

Role definition tasks

- Request a new role definition
- Request changes to a role definition

While the tickets generated by both types of tasks are similar, they do not behave in the same manner, and therefore they are described separately. The ticket functions work the same irrespective of the ticket where you find them, for example a Consult utility works the same even if the ticket type providing the service is different.

As CA RCM is a role management product, many of the features focus on roles. The Role Definition tasks focus on the roles. The CA RCM assumes that user updates will come from a relevant source, such as a Human Resources database. Resource information is collected from the end-points during import.

When a Role Definition task is completed a Requests screen opens. This screen has two tables:

- Attributes
- Links

The next step is to submit all the requests for review by the relevant entity managers. This process is known as an Approval Process.

Self-Service role definition tasks are focused on the system's roles, and the possibility of enrolling users in those roles, assigning them various resources and creating hierarchal connections between different roles, or on the possibility of severing an existing link between a role and another entity. Therefore, during the Approval Process, review tickets are generated for both the role and the linked user/resource/role (hierarchal).

This process is started by the manager who made the Self-Service request (the Self-Service Manager). When an instruction to begin an Approval Process is given, the CA RCM generates a hierarchal Approver Process ticket tree. While for most Self-Service provisioning tasks the ticket tree is generated at once and the task managers and link approvers can work with their tickets directly, Self-Service Role Definition task tickets are generally generated in stages.

Add Role stages

Stage 1: Select Accountable

A Task ticket sent to the Self-Service task manager.

Stage 2: Role Approver

An Add Role ticket sent to the Role manager.

Stage 3: Link Approval Process sub-trees

One Link Entity-Role parent and one Link Entity-Role approver ticket for each request made during the original Self-Service task. The parent ticket is always assigned to the Role manager.

Update Role definition stages

Stage 1: Role Approver

An Update Role ticket sent to the Role manager. This ticket is generated only when a request to Add entities is made.

Stage 2: Approval Process sub-trees

One parent and one approver ticket for each request made during the original Self-Service task. The request can be to either add a link or remove a link between the role and another entity. The parent ticket is always assigned to the Role manager.

The ticket tree generally comprises four families of tickets:

Approval Root ticket

This ticket belongs to the Self-Service manager. Each approval process has only one root ticket.

Main Request Parent ticket

This ticket type depends on the type of request made during the role definition task. There are two possible sources for this ticket:

Add Role Parent ticket

When a new role is generated, this is the main parent ticket. Below it you will find the Task ticket used to select the role's accountable, the role managers' approver ticket and the set of subtrees generated for each request listed in the original Requests table.

Update Role Parent ticket

When a request is made to update a role definition, this ticket is the main parent ticket. Below it you will find the role managers' approver ticket and the set of subtrees generated for each request listed in the original Requests table.

Request Parent Ticket

This ticket is of the same type as the Approver tickets associated with it. This ticket belongs to the Role manager. This node is the parent of the actual approval process Approver tickets that are sent to the Approvers. The number of sub-trees of this type present in an approval process tree depends on the number of Self-Service requests being processed.

Approver Tickets

As role definition task tickets are generated in stages, the CA RCM Portal generates on Role Approver ticket for the role manager and a set of sub-trees, one per request, comprising a Request Parent ticket belonging to the Role manager and an Approver ticket that is sent to the user, resource or role (hierarchical) manager. The tickets generated belong to one of the following ticket types:

Link User-Role, Link Role-Resource or Link Role-Role

Generated when adding a link to specific role.

Delete-Link User-Role, Delete-Link Role-Resource or Delete-Link Role-Role

Generated when making a request to sever a specific link to the role.

Add Role

The role manager approver ticket generated when a request is made to add a new role to the configuration.

Update Role

The role manager approver ticket generated when a request to update role definitions is made or in the special case of multi-user requests to enroll users in a role, where the number of users exceeds the system's threshold.

Entity managers are assigned to an Approval Process as approvers based on the link type. For example, for a Delete Link User-Role process, the user's manager and the role's manager will be assigned as approvers. Users can become approvers for other users only if the Approver's name appears in the manager column (of the Universe's Model configuration files) for the specific user. Users can become approvers for Roles and/or Resources only if they are listed in the configuration's RACI presentation under Accountable, this means that a specific user becomes accountable for a specific entity. Therefore, if you are listed as an entity manager, you will receive Approver tickets when an administrator runs an Approval Process involving your assigned entity.

Self-Service managers have overall control of the approval process. They can transfer responsibility of the process to another manager or cancel the process when necessary.

As the Role manager for the role that is under review, you are tasked with reviewing the changes requested by the Self-Service manager. Approval Processes that include adding links between a role and other entities will generate a Role Approver ticket. This ticket summarizes all the requests that are concerned with adding links between your role and other entities. Only if you approve the requests will the CA RCM Portal generate the Entity Approver tickets for these requests. The reason for this is that the system approves only requests regarding links that have been approved by the managers of both of the linked entities. Therefore if you do not approve the request, to add links, the system considers the request to be denied.

In the case of a Role Update request, if the requests included only removing links or they encompassed both adding and removing links, the tickets generated by the request to remove links will still be generated.

As an approver you are tasked with making the decision whether to approve the request to add/sever a link or not. To aid you in the decision making process, you have the ability to consult with other managers.

Important! As several complex procedures are documented in this chapter, it is important to remember that every ticket has a unique ticket ID number that can be used to differentiate between tickets of the same type that deal with the same issue, but have different functionality or purpose.

This section contains the following topics:

[Role Definition Approval Root Ticket](#) (see page 125)

[Role Definition Main Request Parent Ticket](#) (see page 128)

[Add New Role Ticket Tree](#) (see page 133)

[Update Role Ticket Tree](#) (see page 147)

Role Definition Approval Root Ticket

The Self-Service Approval Root-ticket is the root-ticket that appears in the inbox belonging to the manager/administrator who submitted the Self-Service request. When expanded, you can view the tickets generated for the specific Role Definition Approval Process.

As the tickets to be found below the Approval Root ticket depend on the specific role related requests being made, these tickets will be described where relevant. What is important to realize is that the Approval Root ticket provides the same information and functionality both for an Add Role request and an Update Role Definition request.

Note: When the approval process Approver tickets are not generated a Notification ticket appears below a Request Parent ticket.

Click the ticket title to open the Ticket Properties Form in a separate browser window.

In this section you will find information specific to the Approval Root-ticket type for Self-Service provisioning requests.

<Ticket Title>

Approval Root

Title

[*Self-Service Task*] Approval Root Request. For example: Add Role Approval Root Request.

Description

A description of the ticket. It includes The universe name and the source of the request. For example: Approval Root Request - Request was submitted on Universe Portal from Update Role.

This section covers the following topics:

- The Role Definition Approval Root ticket's General functions
- The Role Definition Approval Root ticket's Advanced functions

More information:

[Approval Root Ticket General Functions \(Role Definition\)](#) (see page 126)

[Approval Root Ticket Advanced Functions \(Role Definition\)](#) (see page 127)

Approval Root Ticket General Functions (Role Definition)

The Role Definition Approval Root ticket provides the following General functionality:

Close

Closes the ticket.

Save

Saves the changes made to the ticket.

Delegate

Transfers the ticket tree to another manager.

Escalate

Transfers the ticket tree to another manager.

Start Process

For regular Approval Processes, this button is disabled, as the procedure starts automatically when the tickets arrive in the approvers' Inbox.

Cancel Process

Allows you to manually stop the Approval Process, at any stage.

Acknowledge

This function is disabled until the Approval Process has been completed.

More information:

[Escalate](#) (see page 37)

[Delegate](#) (see page 38)

Approval Root Ticket Advanced Functions (Role Definition)

The Role Definition Approval Root ticket provides the following Advanced functionality:

Add Comment

Manually add a comment to the ticket.

Add Attachment

Add an attachment or URL to the ticket.

View Transaction Log

The transaction log provides a history of the ticket-related actions executed since the creation of the ticket.

View Children

Opens a table which provides you with information concerning all the nodes/leaves that are located below the current ticket. For the Approval Process Root ticket, this means that you can view information concerning the Approval Processes' Main Request Parent ticket.

View Statistic

Provides the status of all the children tickets.

More information:

[Add Comment](#) (see page 32)

[Add Attachment](#) (see page 33)

[View Transaction Log](#) (see page 34)

Role Definition Main Request Parent Ticket

The Main Request Parent ticket is a management ticket, generated by the CA RCM portal for each Role Definition procedure. All the individual tickets and sub-trees that make up the Role Definition Approval Process ticket tree are located beneath this ticket. The number of children tickets changes over the course of the Approval Process. During the first stage there is usually only one child ticket, as the Approval Process moves on and generates the entity Approver tickets the number of children will increase to include the number of discrete requests made during the original Role Definition request plus whatever individual tickets were generated along the way.

The Role Definition Approval Process supports two different Main Request Parent tickets:

Add Role Main Parent ticket

When a new role is generated, this is the main parent ticket. Below it you will find the Task ticket used to select the role's accountable, the role managers' approver ticket and the set of subtrees generated for each request listed in the original Requests table.

Update Role Main Parent ticket

When a request is made to update a role definition, this is the main parent ticket. Below it you will find the role managers' approver ticket and the set of subtrees generated for each request listed in the original Requests table.

Both ticket types provide you with the same management functionality. They differ in the content of the individual Main Parent ticket.

In this section you will find information specific to the Request Parent tickets generated for Self-Service provisioning requests.

<Ticket Title>

According to source of the request: either Add Role or Update Role.

Title

Title [Role]. For example: New Role [Corporate Security]

Description

Description [Role].

For example: Update Role [Organization=Marketing_Dept.]

Use this ticket's functionality when you wish to transfer the approval process tree to the management of another user or to cancel the approval process. You can use the options in the ticket's Advanced section to access additional information concerning the current ticket and its parent and child tickets.

Click the ticket title to open the Ticket Properties Form in a separate browser window.

This section covers the following topics:

- The Role Definition Main Parent ticket's General functions
- The Role Definition Main Parent ticket More Details section
- The Role Definition Main Parent ticket's Advanced functions

More information:

[Main Parent Ticket General Functions \(Role Definition\)](#) (see page 130)

[Main Parent Ticket Details Section](#) (see page 130)

[Main Parent Ticket Advanced Functions \(Role Definition\)](#) (see page 131)

Main Parent Ticket General Functions (Role Definition)

The Role Definition Main Parent ticket provides the following General functionality:

Close

Closes the ticket.

Save

Saves the changes made to the ticket.

Delegate

Transfers the ticket tree to another manager.

Escalate

Transfers the ticket tree to another manager.

Cancel Process

Allows you to manually stop the Approval Process, at any stage.

More information:

[Escalate](#) (see page 37)

[Delegate](#) (see page 38)

Main Parent Ticket Details Section

The More Details>> and <<Less Details buttons, located below the general function buttons, toggle between showing additional data and hiding the same data. The type of data available is the same whether the ticket is an Add Role main parent ticket, or an Update Role main parent ticket. The content of the fields depends on the original Role Definition task being processed.

The Role Fields table refers to the role's rules. This table will have content only when a new role included a rule, or when a rule is added/changed during an update role process.

As the first step in any role definition approval process is to allow the role manager to approve the links added to the role, the Role Links table provides a list of the entities that were listed as Add requests in the Requests table. Requests to remove links are processed separately. This table provides lists for each possible entity:

- Users to add
- Resources to add
- Parent roles to add
- Children roles to add

If any of the options are empty, it will not appear in the table.

This section is informational only.

Note: You cannot access any of the entity cards for the entities listed here.

Main Parent Ticket Advanced Functions (Role Definition)

The Role Definition Main Parent ticket provides the following Advanced functionality:

Add Comment

Manually add a comment to the ticket.

Add Attachment

Add an attachment or URL to the ticket.

View Transaction Log

The transaction log provides a history of the ticket-related actions executed since the creation of the ticket.

View Parent

Opens the current ticket's parent's ticket.

View Initiators

View of list of the users who launched this ticket.

View Children

Opens a table which provides you with information concerning all the nodes/leaves that are located below the current ticket. For the Approval Process Root ticket, this means that you can view information concerning the various Approver Process tickets and sub-subtrees generated during a Role definition Approval Process.

View Role

Opens the role's card. As the approval process focuses on a specific role, this is the card that is available to you at this stage of the process.

More information:

- [Add Comment](#) (see page 32)
- [Add Attachment](#) (see page 33)
- [View Transaction Log](#) (see page 34)
- [View \[Entity\]](#) (see page 34)

View Children (Role Definition Approval Process)

Role Definition Approval Processes proceed in stages. During each stage, the child tickets you can see when you click View Children will change.

During an Add Role approval process, you will be able to see:

Stage 1

Only the Select Accountable task ticket is listed.

Stage 2

Both the Select Accountable task ticket and the Role Approver tickets are listed.

Stage 3

All the Request Parent tickets for each requested link are listed. Note that the new role's manager is the listed owner of these tickets.

Notice the ticket Type for information on what ticket you are currently viewing.

During an Update Role approval process you can see:

Stage 1

The Role Approver ticket is listed.

Stage 2

All the Request Parent tickets for each requested link are listed. Note that the new role's manager is the listed owner of these tickets.

Notice the ticket Type for information on what ticket you are currently viewing.

Click Close Children to close the table.

Add New Role Ticket Tree

This process is started by the manager who made the Self-Service request (the Self-Service Manager). When an instruction to begin an Approval Process is given, the CA RCM generates a hierarchal Approver Process ticket tree. The Self-Service Request a New Role Definition (Add New Role) task tickets are generated in stages.

1: Select Accountable

A Task ticket sent to the Self-Service task manager.

2: Role Approver



An Add Role ticket sent to the Role manager.


3: Link Approval Process sub-trees

One Link Entity-Role parent and one Link Entity-Role approver ticket for each request made during the original Self-Service task. The parent ticket is always assigned to the Role manager.

The Add New role ticket tree is constructed as follows:





Stage 1:

Ticket	Description
 Approval Root ticket	This ticket is identical to other Approval Process Approval Root tickets. For more information see Self-Service Approval Root Ticket (see page 125)
 Self-Service Main Request Parent Ticket	An Add Role parent ticket sent to the Self-Service task manager. For more information see Role Definition Main Request Parent Ticket (see page 130)

 Select Accountable	A Task ticket sent to the Self-Service task manager. For more information see Select Accountable Ticket (Add New Role) (see page 135).
--	--

After the Self-Service task manager has selected a person who will be accountable for this role (stage 1), stage 2 begins and a new ticket is generated:






Stage 2:

Ticket	Description
 Approval Root ticket	Same ticket.
 Self-Service Main Request Parent Ticket	Same ticket
 Select Accountable	This Task ticket has been completed and is currently archived
 Approver Ticket	The Role Approver ticket. This is an Add Role approver ticket. It is sent to the Role manager. It contains all the requests to add a link between the new role and other entities. For more information see Role Approver Ticket (Add Role) (see page 139).

Note: If the role manager rejects the request submitted in the Role Approver ticket, the Approval Process ends and the relevant emails and info-tickets are generated.

After the Role manager has approved the enrollment of all the users in the Approver ticket, stage 3 begins and a new set of tickets is generated.

Stage 3 (Includes examples of possible Request sub-trees for an Add Role ticket tree):

Ticket	Description
 Approval Root ticket	Same ticket.
 Self-Service Main Request Parent Ticket	Same ticket
 Select Accountable	This Task ticket has been completed and is currently archived
 Approver Ticket	This Role Approver ticket has been completed and is now archived
 Self-Service Request Parent	A Link User-Role parent ticket

ticket



Approver Ticket

Only one ticket. A Link User-Role approver ticket



Self-Service Request Parent

A Link Role-Resource parent ticket

ticket



Approver Ticket

Only one. A Link Role-Resource approver ticket

The number of Link User-*[Entity]* sub-trees depends on the number of role-entity requests that were originally submitted. If a request was made to enroll 10 users to a role, then there will be 10 Link User-Role subtrees generated during the third stage of the Add New Role Approval Process.

The Link Entity-Role parent and approver tickets are standard tickets.

More information:

[Introducing the Requests Table](#) (see page 118)

[Self-Service Request New Role Parent Ticket](#) (see page 142)

[Self-Service Request New Role Approver Ticket](#) (see page 145)

Select Accountable Ticket (Add New Role)

One of the advantages of the CA RCM is its ability to take advantage of RACI presentation techniques. When a request for a new role is generated, the first thing that the CA RCM Portal does is to generate a Task ticket that aids the Self-Service manager in swiftly setting the new role's Accountable (Approver).

The Select Accountable Task ticket follows standard CA RCM Portal ticket guidelines.

In this section you will find information specific to the Select Accountable Task ticket.

<Ticket Title>

Task

Title

Select Accountable to Role [Role Name]. For example: Select Accountable to Role [Corporate Security]

Description

Instructions: To continue please choose an accountable user to Corporate Security role [GENTKT039]

The More Details>>/<<Less Details option provides far more information than in other parent tickets. In this case you can see here a full list of the ID numbers for all the users that you (or the Self-Service manager) requested to enroll in this role.

This section covers the following topics:

- Select Accountable (Function)
- Select Accountable Ticket General Functions
- Select Accountable Ticket Advanced Functions
- View Violations

More information:

[Select Accountable \(Function\)](#) (see page 136)

[Select Accountable Ticket General Functions](#) (see page 137)

[Select Accountable Ticket Advanced Functions](#) (see page 138)

[View Violations](#) (see page 139)

Select Accountable (Function)

This purpose of the Select Accountable Task ticket is to select the role's manager, the user who will act as the Approver whenever a request is made that is connected to this role.

At first, the Role Accountable field is empty (located under More Details>>). The Continue button is disabled until a user is selected.

When you click Select Accountable, the Choose Accountable for New Role screen opens in a separate browser window.

The Choose Accountable for New Role screen is divided into two sections:

The filter

Located in the window's header. The filter lets you narrow down the list of proposed approvers.

The proposed users

This table presents a pre-filtered list of users who can become Approvers. This list can be filtered to aid in finding a specific user.

After selecting a user as the role's Approver, the Continue button is enabled. The new role manager is listed under the More Details section of the Select Accountable Task ticket.

Click Continue to go to the next stage of the Add New Role Approval Process.

More information:

[Filter a Data Table](#) (see page 16)

[Select Accountable Ticket General Functions](#) (see page 137)

Select Accountable Ticket General Functions

The Select Accountable Task ticket (for the Self-Service Request Add New Role task) provides the following General functionality:

Close

Closes the ticket.

Save

Saves the changes made to the ticket.

Delegate

Transfers the ticket tree to another manager.

Escalate

Transfers the ticket tree to another manager.

Select Accountable

Provides the new role's accountable. After an accountable is selected the Continue button is enabled.

Continue

This button is disabled until an Accountable is selected. Click to continue to stage 2 of the Add New Role Approval Process.

More information:

[Delegate](#) (see page 38)

[Escalate](#) (see page 37)

[Select Accountable \(Function\)](#) (see page 136)

Select Accountable Ticket Advanced Functions

The Select Accountable Task ticket (for the Self-Service Request Add New Role task) provides the following Advanced functionality:

Add Comment

Manually add a comment to the ticket.

Add Attachment

Add an attachment or URL to the ticket.

View Transaction Log

The transaction log provides a history of the ticket-related actions executed since the creation of the ticket.

View Parent

Opens the current ticket's parent's ticket.

View Initiators

View of list of the users who launched this ticket.

View Role

Opens the Role's card. Because the review is limited to the role in this view, you cannot access the users' cards.

View Violations

View the list of violations.

More information:

[Add Comment](#) (see page 32)

[Add Attachment](#) (see page 33)

[View Transaction Log](#) (see page 34)

[View \[Entity\]](#) (see page 34)

[View Violations](#) (see page 139)

View Violations

A violation is a breach of corporate security policies, guidelines, BPRs and/or regulations. When you decide whether to approve or reject a request to create a link between a role and other entities within a Role Definitions Approver Process Approver ticket, you can check whether there are any violations connected to the Self-Service request you are examining.

When you click a violation, the Violations Information window in a separate browser window.

Click Close to close the window.

You can use this utility to view a list of the violations connected with the link(s) under review.

There are three fields:

Name

The violation title.

Description

Provides the details of the violation

Score

The score as listed when the BPR was first generated.

Click View Violations to view the View Violations screen in a separate browser window. Click Close to close the browser window.

Role Approver Ticket (Add Role)

The second stage of the Add New Role Approver Process starts after you have selected an user as the role's accountable and clicked Continue. A Role Approver ticket is generated. This Approver ticket is sent to the new role's manager. It contains a table listing all the links that were requested during the Request New Role Definition task.

Once the role manager approves the link requests listed in this ticket, stage three of the Add New Role Approval Process begins and a new set of Approver tickets is generated. This includes one sub-tree for every requested link that consists of parent-child pairs of tickets, where the parent ticket is a standard Link Entity-Role Parent ticket and the child ticket is a standard Link Entity-Role Approver ticket.

The Role Approver ticket supplies you with all the data you need to make the decision whether to approve or reject the request. The Role Approver ticket also provides you with the required functionality to assist you in the process.

More information:

[Self-Service Request New Role Parent Ticket](#) (see page 142)
[Self-Service Request New Role Approver Ticket](#) (see page 145)
[Approve](#) (see page 31)
[Reject](#) (see page 31)
[Role Approver Ticket General Functions](#) (see page 140)
[Role Approver Ticket Advanced Functions](#) (see page 141)

Role Approver Ticket General Functions

The Role Approver ticket provides the following General functionality:

Close

Closes the ticket.

Save

Saves the changes made to the ticket.

Delegate

Delegates the ticket tree to a sub-administrator.

Escalate

Escalates the ticket tree to a supervising manager.

Consult

Allows you to request a consult from one or more managers. When you activate this service, a View Consult Results button appears in the Advanced functions section of the Ticket Properties Form.

Approve

Approve the Self-Service request. In this case, this leads to the second stage of the Approval Process, where the user review Approval Process sub-trees are generated and the Approver tickets are sent to the user managers.

Reject

Reject the Self-Service request.

Note: It is important to remember that when reviewing a Role Approver ticket, you can either accept the request for ALL listed users, enrolling all of them, or you can reject the request for ALL users.

More information:

[Escalate](#) (see page 37)
[Delegate](#) (see page 38)
[Approve](#) (see page 31)
[Consult](#) (see page 35)
[Reject](#) (see page 31)

Role Approver Ticket Advanced Functions

The Role Approver ticket provides the following Advanced functionality:

Add Comment

Manually add a comment to the ticket.

Add Attachment

Add an attachment or URL to the ticket.

View Transaction Log

The transaction log provides a history of the ticket-related actions executed since the creation of the ticket.

View Parent

Opens the current ticket's parent's ticket.

View Initiators

View of list of the users who launched this ticket.

View Violations

View the list of violations.

View Role

This button is disabled because all the role's details already appear in this ticket.

View Consult Results

This button appears only when the Consult service has been activated.

More information:

[Add Comment](#) (see page 32)

[Add Attachment](#) (see page 33)

[View Transaction Log](#) (see page 34)

[View Violations](#) (see page 139)

[View Consult Results](#) (see page 36)

Self-Service Request New Role Parent Ticket

The Self-Service Request New Role Parent ticket is a management ticket generated by the CA RCM portal during the third stage of the Add New Role Approval Process. While the Approval Root ticket controls the lifecycle of the whole tree, the New Role Request Parent ticket controls the lifecycle of the approver ticket generated during the third stage of the Approval.

The ticket's type is the same as the Approver ticket below it, but it is intended to be a management ticket. The ticket owner in this case is the role manager.

In this section you will find information specific to the Self-Service Request New Role Parent ticket.

<Ticket Title>

Link [Entity] Role

Title

Request to add [Entity] to role association. Role: [Role], [Entity]: [Entity ID]. For example: Request to add user to role association. role:'Corporate Security',user:'89213720'

Description

Request to add [Entity] to role association. Role: [Role], [Entity]: [Entity ID] -Request was submitted on Universe [Universe] from [Self-Service Task]. For example: Request to add user to role association. role:'Corporate Security',user:'89213720' - Request was submitted on Universe Portal from Add Role.

The More Details>>/<<Less Details option provides additional information.

Use this ticket's functionality when you wish to transfer the specific sub-tree to the management of another user or to cancel this specific review. You can use the options in the ticket's Advanced section to access additional information concerning the current ticket and the Approver ticket associated with it in the sub-tree.

New Role Parent Ticket General Functions

The Self-Service Request Update Role Parent ticket provides the following General functionality:

Close

Closes the ticket.

Save

Saves the changes made to the ticket.

Delegate

Transfers the ticket tree to another manager.

Escalate

Transfers the ticket tree to another manager.

Cancel Process

Allows you to manually stop the Approval Process, at any stage.

More information:

[Escalate](#) (see page 37)

[Delegate](#) (see page 38)

New Role Parent Ticket Advanced Functions

The Request New Role Parent ticket provides the following Advanced functionality:

Add Comment

Manually add a comment to the ticket.

Add Attachment

Add an attachment or URL to the ticket.

View Transaction Log

The transaction log provides a history of the ticket-related actions executed since the creation of the ticket.

View Parent

Opens the current ticket's parent's ticket.

View Initiators

View of list of the users who launched this ticket.

View Children

Opens a table which provides you with information concerning the leaf that is located below the current ticket. For the Request Parent ticket, this means that you can view information concerning the link's Approver ticket.

View Role

Opens the Role's card.

View [Entity]

The Add New Role Approver tickets review links between the new role and other entities. This button will provide you with the entity card associated with the entity to be linked to the new role.

More information:

[Add Comment](#) (see page 32)

[Add Attachment](#) (see page 33)

[View Transaction Log](#) (see page 34)

[View \[Entity\]](#) (see page 34)

Self-Service Request New Role Approver Ticket

During the third stage of an Add New Role Approval Process, after the role manager has approved the suggested links to the new role, a new set of Approver tickets is generated. These tickets are standard Link [Entity]-Role Approver tickets, one for each link requested during the Request New Role Definition task.

The New Role Approver ticket supplies you with all the data you need to make the decision whether to approve or reject the Role definition request. The Approver ticket also provides you with the required functionality to assist you in the process.

More information:

[Reject](#) (see page 31)

[Approve](#) (see page 31)

[New Role Approver Tickets' General Functions](#) (see page 145)

[New Role Approver Tickets Advanced Functions](#) (see page 146)

New Role Approver Tickets' General Functions

The Self-Service provisioning Approver ticket provides the following General functionality:

Close

Closes the ticket.

Save

Saves the changes made to the ticket.

Delegate

Transfers the ticket tree to another manager.

Escalate

Transfers the ticket tree to another manager.

Consult

Allows you to request a consult from one or more managers. When you activate this service, a View Consult Results button appears in the Advanced functions section of the Ticket Properties Form.

Approve

Approve the Self-Service request.

Reject

Reject the Self-Service request.

More information:

[Delegate](#) (see page 38)

[Escalate](#) (see page 37)

[Consult](#) (see page 35)

[Approve](#) (see page 31)

[Reject](#) (see page 31)

New Role Approver Tickets Advanced Functions

The Approver ticket provides the following Advanced functionality:

Add Comment

Manually add a comment to the ticket.

Add Attachment

Add an attachment or URL to the ticket.

View Transaction Log

The transaction log provides a history of the ticket-related actions executed since the creation of the ticket.

View Parent

Opens the current ticket's parent's ticket.

View Initiators

View of list of the users who launched this ticket.

View Violations

This button is disabled.

View [Entity]

Opens the entity's card. Two buttons are provided, one for each side of the link under review.

View Consult Results

This button appears only when the Consult service has been activated.

More information:

[Add Comment](#) (see page 32)

[View Transaction Log](#) (see page 34)

[Add Attachment](#) (see page 33)

[View \[Entity\]](#) (see page 34)

[View Consult Results](#) (see page 36)

Update Role Ticket Tree

The Update Role Ticket tree is generated following one of two tasks:




- In the case of where a request is made to update a role's definitions, when the Self-Service manager made a request to add links to the specific role. When only requests to remove links have been made, the Update Role ticket tree that is generated follows the standard format for other Self-Service ticket trees.
- In the special case of Manage My Team's Role Assignments, when the number of users selected to enroll in a role is greater than the system threshold, a different set of tickets is generated.

The system threshold is set in the `eurekify.properties` file and is governed by the property filter:

```
approvals.configuration.updateRole.minimumLinks = 4
```




The ticket tree in this case is constructed as follows:

Stage 1:






Ticket	Description
 Approval Root ticket	This ticket is identical to other Approval Process Approval Root tickets.
 Self-Service Main Request Parent Ticket	An Update Role parent ticket
 Approver Ticket	The Role Approver ticket. This is an Update Role approver ticket. It is sent to the Role manager. It contains all the requests to add a link between the new role and other entities. For more information see Self-Service Request Update Role Approver Ticket (see page 151)

After the Role manager has approved the enrollment of all the users in the Approver ticket, stage 2 begins and a new set of tickets is generated.

Stage 2:

Ticket	Description
 Approval Root ticket	This ticket is identical to other Approval Process Approval Root tickets.
 Self-Service Main Request Parent Ticket	An Update Role parent ticket.
 Approver Ticket	Only one. An Update Role approver ticket.

The following sub-trees are examples of possible Request sub-trees for an Update Role ticket tree:

Ticket	Description
 Approver Ticket	This Role Approver ticket has been completed and is now archived
 Self-Service Request Parent ticket	A Link User-Role parent ticket
 Approver Ticket	Only one. A Link User-Role approver ticket
 Self-Service Request Parent ticket	A Remove Link Role-Resource parent ticket
 Approver Ticket	Only one. A Remove Link Role-Resource approver ticket

Note: If the Self-Service request included removing links, the sub-trees generated in stage 2 will include Remove Entity-Link type tickets.

The number of Remove Link/Link User-Role subtrees depends on the number of entity-role requests that were originally submitted. If a request was made to enroll 10 users to a role, then there will be 10 Link User-Role subtrees generated during the second stage of the Self-Service Approval Process.

The Remove Link/Link User-Role parent and approver tickets are standard tickets.

More information:

- [CA RCM Properties](#) (see page 259)
- [Updating Role Definitions](#) (see page 117)
- [Running Self-Service Tasks](#) (see page 81)
- [Manage My Team's Role Assignments](#) (see page 87)
- [Self-Service Request New Role Parent Ticket](#) (see page 142)
- [Self-Service Request New Role Approver Ticket](#) (see page 145)

Self-Service Request Update Role Parent Ticket

The Self-Service Request Update Role Parent ticket is a management ticket generated by the CA RCM portal when a request made using the business process *Managing My Team's Roles* involves a number of users that exceeds the system threshold. While the Approval Root ticket controls the lifecycle of the whole tree, the Update Role Request Parent ticket controls the lifecycle of the approver ticket generated during stage 1 of the Approval Process and also all the sub-trees generated during stage 2 of the Approval Process.

In this section you will find information specific to the Self-Service Request Update Role Parent ticket.

<Ticket Title>

Update Role

Title

Update Role [*Role Name*]

Description

Update Role [*Role Name*]

The More Details>>/<<Less Details option provides more information than in other parent tickets. In this case you can see a full list of the ID numbers for all the users that you (or the Self-Service manager) requested to enroll in this role.

Use this ticket's functionality when you wish to transfer the specific link's sub-tree to the management of another user or to cancel this specific review. You can use the options in the ticket's Advanced section to access additional information concerning the current ticket and the rest of the tickets in the sub-tree.

Update Role Ticket General Functions

The Self-Service Request Update Role Parent ticket provides the following General functionality:

Close

Closes the ticket.

Save

Saves the changes made to the ticket.

Delegate

Transfers the ticket tree to another manager.

Escalate

Transfers the ticket tree to another manager.

Cancel Process

Allows you to manually stop the Approval Process, at any stage.

More information:

[Delegate](#) (see page 38)

[Escalate](#) (see page 37)

Update Role Parent Ticket Advanced Functions

The Request Parent ticket provides the following Advanced functionality:

Add Comment

Manually add a comment to the ticket.

Add Attachment

Add an attachment or URL to the ticket.

View Transaction Log

The transaction log provides a history of the ticket-related actions executed since the creation of the ticket.

View Parent

Opens the current ticket's parent's ticket.

View Initiators

View of list of the users who launched this ticket.

View Children

Opens a table which provides you with information concerning all the nodes/leaves that are located below the current ticket. For the Request Parent ticket, this means that you can view information concerning the link's Approver tickets.

View Role

Opens the Role's card. In this case the review is limited to the role and you cannot access the users' cards.

More information:

[Add Comment](#) (see page 32)

[View Transaction Log](#) (see page 34)

[Add Attachment](#) (see page 33)

[View \[Entity\]](#) (see page 34)

Self-Service Request Update Role Approver Ticket

When a Self-Service multi-user request of the type Manage My Team's Roles is generated, and the number of users exceeds the CA RCM Portal's threshold, an Update Role Approver ticket is generated in the first stage of the Approval Process. Once the role manager approves the enrollment of the users listed in the ticket in the role, a new set of Approver tickets is generated. This second set of sub-trees consists of parent-child pairs of tickets, where the parent ticket is a standard Link User-Role Parent ticket and the child ticket is a standard Link User-Role Approver ticket.

The Update Role Approver ticket supplies you with all the data you need to make the decision whether to approve or reject the Self-Service provisioning request. The Approver ticket also provides you with the required functionality to assist you in the process.

More information:

[Self-Service Request New Role Parent Ticket](#) (see page 142)

[Self-Service Request New Role Approver Ticket](#) (see page 145)

[Approve](#) (see page 31)

[Reject](#) (see page 31)

[Update Role Approver Tickets' General Functions](#) (see page 152)

[Update Role Approver Tickets Advanced Functions](#) (see page 153)

Update Role Approver Tickets' General Functions

The Self-Service provisioning Approver ticket provides the following General functionality:

Close

Closes the ticket.

Save

Saves the changes made to the ticket.

Delegate

Transfers the ticket tree to another manager.

Escalate

Transfers the ticket tree to another manager.

Consult

Allows you to request a consult from one or more managers. When you activate this service, a View Consult Results button appears in the Advanced functions section of the Ticket Properties Form.

Approve

Approve the Self-Service request. In this case, this leads to the second stage of the Approval Process, where the user review Approval Process sub-trees are generated and the Approver tickets are sent to the user managers.

Reject

Reject the Self-Service request.

Note: It is important to remember that when reviewing an Update Role Approver ticket, you can either accept the request for ALL listed users, enrolling all of them, or you can reject the request for ALL users.

More information:

[Escalate](#) (see page 37)

[Delegate](#) (see page 38)

[Consult](#) (see page 35)

[Approve](#) (see page 31)

[Reject](#) (see page 31)

Update Role Approver Tickets Advanced Functions

The Approver ticket provides the following Advanced functionality:

Add Comment

Manually add a comment to the ticket.

Add Attachment

Add an attachment or URL to the ticket.

View Transaction Log

The transaction log provides a history of the ticket-related actions executed since the creation of the ticket.

View Parent

Opens the current ticket's parent's ticket.

View Initiators

View of list of the users who launched this ticket.

View Violations

View the list of violations.

View [Entity]

Opens the entity's card. Two buttons are provided, one for each side of the link under review.

View Consult Results

This button appears only when the Consult service has been activated.

More information:

[Add Comment](#) (see page 32)

[Add Attachment](#) (see page 33)

[View Transaction Log](#) (see page 34)

[View \[Entity\]](#) (see page 34)

[View Violations](#) (see page 139)

[View Consult Results](#) (see page 36)

Chapter 9: Entity Browser

The Entity Browser screen lets you view details of a configuration.

The Entity Browser initially displays the following fields:

Universe

Specifies the universe from which you select a configuration. Select the All option to view all configurations in the database.

Configuration

Specifies the configuration you want to browse.

Use these fields to select a configuration. The following tabs appear:

Users

Displays a table of users in the configuration, and basic attribute values. You can customize the table by adding additional attribute columns.

Click on a user to [view its details](#) (see page 156).

Roles

Displays a list of roles in the configuration, and basic attribute values. You can customize the table by adding additional attribute columns.

Click on a role to [view its details](#) (see page 156).

Resources

Displays a list of resources in the configuration, and basic attribute values. You can customize the table by adding additional attribute columns.

Click on a resource to [view its details](#) (see page 156).

Statistics

Displays the number of entities and links in the configuration.

Organization Chart

Displays a [configurable tree](#) (see page 157) of the user and manager hierarchy of the configuration.

This section contains the following topics:

[User, Role, and Resource Details](#) (see page 156)

[Modify the Organization Chart](#) (see page 157)

User, Role, and Resource Details

When you click a user, role, resource, or account in the entity browser, a popup window shows details for that entity. The window can contain the following tabs, depending on the type of entity you are examining:

Users

Displays the users that link to the entity.

Roles

Displays the roles that link to the entity.

Sub Roles

Displays the child roles of the role.

Parent Roles

Displays the parent roles of the role.

Resources

Displays the resources that link to the entity. When the target universe includes usage data from a CA Enterprise Log Manager instance, you can specify Usage View to display this usage data in this tab.

Accounts

Displays the user accounts on external endpoints that link to the entity. This tab only appears if the target universe contains account configurations.

Approvals

Displays the approval tasks of the user in currently active campaigns.

RACI

Displays the users linked to the entity by RACI analysis of the configuration.

Modify the Organization Chart

The Organization Chart tab of the entity browser displays the users in the target configuration in a clickable tree. Each level of the tree groups users based on the value of a user attribute in the target configuration.

You can configure the levels of the tree to show users in various ways. For example, you can create a tree that shows geographical distribution of users. You can also create a tree that shows the management structure of the organization.

Note: When you modify the organization chart, you change only the display of users in the tree. You do not change any user data in the configuration.

To modify the organization chart

1. In the entity browser, click the Organization Chart tab.
2. In the Select Fields area of the tab, specify the user attribute that sorts the top level of the tree in the Level 1 drop-down list.
3. Specify the user attribute that sorts the next level of the tree in the Level 2 drop-down list.
4. Continue to specify levels of the tree:
 - To add more levels, click the plus icon at the lowest level of the tree.
A new drop-down list appears.
 - To delete a level, click the minus icon beside that level.
The drop-down list is removed, and lower levels are renumbered.
5. Click Update Organization Chart.
The tree display reflects the structure you specified.

Chapter 10: How to Generate Reports

Reports provide customized views of role-based configurations you create in CA RCM. Generate reports to:

- Track the progress of import/export, role definition, or certification campaigns.
- Analyze role hierarchies and user/resource assignments in detail.
- Share management-level information on role-based access control and compliance activities.

CA RCM provides a range of predefined report types, which can be customized by specifying filter, sorting, and threshold parameters.

The following table describes the steps to generate a report in CA RCM:

Step	Refer to...
1. Select a report to run.	Report Types (see page 160)
2. Select data files, specify customization parameters, and generate the report.	Parameters and Filters for Report Generation (see page 161)
3. View the report in your browser.	Display a Report's Index (see page 164)and Change Report Parameters (see page 164)
4. Export the report to a file, or print it.	Export a Report to a File (see page 164)or Print a Report (see page 165)

This section contains the following topics:

- [Report Types](#) (see page 160)
- [Parameters and Filters for Report Generation](#) (see page 161)
- [Display a Report's Index](#) (see page 164)
- [Change Report Parameters](#) (see page 164)
- [Export a Report to a File](#) (see page 164)
- [Print a Report](#) (see page 165)

Report Types

Reports are accessed from the CA RCM portal by choosing Reports from the main menu.

Reports are grouped into the following categories:

- Configuration Reports - detailed listings of users, resources, or roles, and their links to other entities. These reports let managers review in detail the privileges assigned to users or resources under their responsibility.
- Privileges Quality Management - graphical presentations of the most common, significant pattern-based analytical metrics of the configuration (similar to those used during the audit phase of role management). These reports give a quick, visual indication of how well the current role hierarchy matches usage patterns, and what proportion of users have suspect patterns of access.
- Role Management - reports used to analyze the role hierarchy, and perform before/after and what-if comparisons of different configurations.
- Policy Management - reports used to verify use of Business Process Rules (BPRs).
- Campaigns - reports used to track the progress of certification campaigns, and summarize changes made during a campaign.

Parameters and Filters for Report Generation

To generate a report, you must specify the configuration file or universe on which to base the report. You may have to specify other parameters for some reports.

You can also specify parameters that filter the report contents. This allows you to limit the report to specific data sets based on user account attributes, geographic location, network structure, or organization/business unit. Additional parameters let you control the sorting of records in some reports, or set statistical thresholds for charts and graphs.

The following parameters are used to generate reports. Not all parameters are used for every report.

Configuration

Specifies the configuration file upon which the report will be based. The drop-down lists all configuration files in the CA RCM database.

Use the following parameters to filter the report based on user, role, or resource attributes:

by Field

Specifies a data field in the configuration file that is used to filter and sort records. The drop-down shows existing data fields in the configuration file specified by the **Configuration** parameter. Only relevant data fields are shown - for example, only user attributes are shown for reports organized by user account.

From/To

Specifies the range of records to include in the report based on the data field specified in the **by Field** parameter. The drop-downs show existing field values drawn from the specified configuration file.

Pattern

Defines a pattern-matching string that selects records from the specified configuration file to include in the report. The string is applied as a filter to the data field specified in the **by Field** parameter. The pattern must follow the usage defined for the `java.util.regex.Pattern` class in the Java version supported by this release.

Use the following parameters when working with analytical/statistical reports based on the selected configuration's audit card:

Audit Card

Specifies the audit card from which analytical information will be drawn to generate the report. The drop-down lists all audit cards associated with the specified configuration file.

Min Score

Specifies a threshold for including information in the report. This filter is applied to the audit card specified by the **Audit Card** parameter. Audit criteria with a score lower than the threshold are not included in the report. Use this filter to exclude audited conditions that are not prevalent or significant in the specified configuration.

From Alert ID/To Alert ID

Specifies a range of Alert IDs to include in the report. The drop-downs show existing Alert ID values in the audit card specified by the **Audit Card** parameter.

Alert Type

Specifies an analytical alert that is used as a filter. Only alerts of the type specified are included in the report. The drop-down shows all the standard analytical alerts that are present in the audit card specified by the **Audit Card** parameter.

From Date/To Date

Specify a time-based filter for audit card data. The report includes only analytical alerts that were recorded in the specified time frame. This filter is applied to the audit card specified by the **Audit Card** parameter.

Use the following parameter with the Policy Verification Report for business rules:

Policy

Specifies a Business Policy Rule (BPR) file used to filter report data. Only alerts related to the specified BPR are included in the report. The drop-down shows all BPR files in the CA RCM database.

Use the following parameters with the Role Modeling Methodologies Comparison report:

Master Configuration

Specifies the configuration used as a reference in comparing several configurations. The drop-down shows all configuration files in the database.

Master Configuration Label

Defines a text label for the reference configuration.

Configuration *n*

Specifies a configuration that is compared to the master configuration. The drop-down shows all configuration files in the database.

Label

Defines a text label for the corresponding configuration.

Use the following parameters when working with campaign-related reports:

Campaign

Specifies the campaign the report will reference. The drop-down lists all campaigns defined in the portal.

All Approvers

All participants who must approve privileges for users or resources they manage are included in the report.

Select by Field

Specifies a user attribute field used to select participants. The drop-down shows all user attributes defined in the campaign's affiliated configuration file. Select an attribute, and existing values in the configuration file are listed. Click a value to use it as a filter. Only participants with that attribute value are included in the report.

Use the following parameters with the Life Cycle Report:

Universe

Specifies the universe the report will reference. The drop-down lists all universes defined in the portal.

Configurations

Specifies the configurations in the universe to use for the report.

Entity Type

Specifies the entity the report will cover.

by Field

Specifies a data field used to filter participants. The drop-down shows all data fields defined for the selected entity type in the specified configuration file(s). Select an attribute, and existing values are listed. Click a value to use it as a filter.

From Date


Specifies the report's start date. Changes to selected entities since this date are included in the report.

Show Current Links

Includes existing links to other entities in the report.

Display a Report's Index

Some reports are indexed by the data field used to filter and sort the report. You can use this index to navigate the report in your browser.

To display a report's index, click . A navigation pane appears on the left of the screen.

Change Report Parameters

You can regenerate the report with different parameter settings. This is useful if the scope of the report is not what you planned, or if you wish to compare parallel subsets of information - for example, different locations or business units.

To regenerate the report


1. Click the Show Parameters link on the left of the report display.
The parameters dialog for this report opens, with current settings displayed.
2. Change any parameter settings you wish, and click OK.
The same report is generated, using the new settings.

Note: The previous version of the report is overwritten. To save the older version, print or export it before you regenerate the report with new parameters.

Export a Report to a File

You can save reports in several common formats. This allows you to share them with others and include them in other documents.


To export a report to a file

1. Click  on the left side of the window.
The Export Report dialog appears.
2. Select the document format, output range, and sizing options. Click **OK**.
A prompt appears when the document is generated.
3. Do one of the following:
 - Choose **Save** to save the file.
 - Choose **Open** to view the file.

Print a Report

You can send reports to a printer to share or archive information, or to simplify review of longer-format reports.

To print a report

1. Click  on the left side of the report window.
The Print Report dialog appears.
2. Choose an output format and print range, and click OK.
A print preview appears in a new browser window.
3. Configure printer settings and print.

Chapter 11: Editing Business Process Rules

This section contains the following topics:

[Business Process Rule Concepts](#) (see page 167)

[How to Work with Business Policies in the CA RCM Portal](#) (see page 168)

Business Process Rule Concepts

A Business Process Rule (BPR) expresses business, provisioning, or security constraints as a logical condition that can be applied to the entities and links in a CA RCM configuration. Consider the following example:

<Purchasing> **forbidden to be** <Subcontractor Payments>

You can apply this statement to a CA RCM configuration to help ensure that workers, with privileges to order stock from subcontractors, do not have roles with privileges to issue checks to those subcontractors.

Typically a BPR is defined by specifying the following information:

- The type of rule—CA RCM provides a broad range of rules that let you examine and compare various entity values. The role type used in the example mentioned previously is Restrict access of users to roles by role access. This type of rule restricts the roles a user can have based on other roles they already have.
- The logical condition—in our example, users with certain roles are forbidden from having other roles. But you can also use this type of rule to allow or require users with certain roles to have other roles.
- Data sets and limit values—in our example, we define a set of roles related to purchasing functions, and another set of roles that grant payment privileges.

A Business Policy is a set of BPRs. This policy (saved as a .bpr document) exists independently of any specific configuration. The rules that comprise the policy can be adapted and applied to any CA RCM configuration to verify its logic, integrity and compliance with policy.

More information:

[Business Process Rule Types](#) (see page 172)

How to Work with Business Policies in the CA RCM Portal

Follow these general procedures when you work with BPR files in the CA RCM portal interface.

Note: You can also work with BPR files using the DNA client application. There are several differences between the two editing interfaces. For example, in the DNA interface you can specify groups of entities by selecting them from an open configuration file. In the portal interface, a wizard simplifies rule editing. You can also use the Data Manager application to import BPR files into the database. For more information about BPR editing in DNA, see the *DNA Users Guide* and the *Data Manager User Guide* for this release.

To access BPR tools, click Administration, BPR Management from the portal main menu.

The BPR list screen appears. The table lists all business policy files in the database.

From this screen, you can perform the following actions:

- To create a business policy file click Create New.
- To edit an existing business policy file click Edit beside the file you want to edit.
- To run an existing business policy file on a configuration, click Run.
- To remove a business policy file from the database, click Delete beside the file you want to remove.

Run Business Policy Files from the CA RCM Portal

When you apply a business policy file to a configuration, CA RCM analyzes the configuration to find entities and links that violate the rules of the policy. The result is an audit card that contains all violations of policy that were found in the configuration.

To run business policy files from the CA RCM portal

1. Click Administration, BPR Management from the portal main menu.

The BPR list screen appears. The table lists all business policy files in the database.

2. Click Run.

The Run BPRs screen appears.

3. Specify values for the following fields:

Audit Card

Defines the name of the audit card that contains any violations found in the target configuration.

Configuration

Specifies a configuration file in the database that is the target for business policy analysis.

4. In the Select BPRs area of the screen, select the business policy files you want to apply to the target configuration.
5. Click Run.

The audit card is created, and analysis of the configuration file begins. If no violations are found, the empty audit card is deleted from the database.

Create a Business Policy File from the CA RCM Portal

You can change various settings of business policy file, or edit the policy rules in the file.

To create a business policy file from the CA RCM Portal

1. Click Administration, BPR Management from the portal main menu.
The BPR list screen appears. The table lists all business policy files in the database.
2. Click Create New.
The Create BPR screen appears.
3. Specify settings for the policy. The following field is not self-explanatory:

Reference Configuration

The configuration used to create and test the policy file.

Note: Business policy files are independent of configuration files. The reference configuration is only used to create and test the policy file. You can apply the finished business policy to any configuration.

4. Specify optional behaviors for the policy file in the Policy Attributes area of the screen. Options include:

Read Only

Specifies whether file is editable.

Logged

Specifies whether changes to the file are recorded in the Transaction log.

Completed

This field not currently used.

5. Click Save.
The business policy file is created in the database.
The Edit BPR screen appears.
6. Use the [editing tools of this screen](#) (see page 170) to define and modify rules in the policy file.

More information:

[Edit a Business Policy File from the CA RCM Portal](#) (see page 170)

Edit a Business Policy File from the CA RCM Portal

You can change various settings of business policy file, or edit the policy rules in the file.

To edit a business policy file from the CA RCM Portal

1. Click Administration, BPR Management from the portal main menu.
The BPR list screen appears. The table lists all business policy files in the database.
2. Click Edit beside the file you want to edit.
The Edit BPR screen appears.
3. Modify settings for the policy. The following fields are not self-explanatory:

Reference Configuration

The configuration used to create and test the policy file.

Note: Business policy files are independent of configuration files. The reference configuration is only used to create and test the policy file. You can apply the finished business policy to any configuration.

4. Specify optional behaviors for the policy file in the Policy Attributes area of the screen. Options include:

Read Only

Specifies whether file is editable others.

Logged

Specifies whether changes to the file are recorded in the Transaction log.

Completed

This field not currently used.

5. The table in the center of the screen lists rules in the policy. To modify the rules, perform one of these actions:
 - Click Add Rule to [create a rule](#) (see page 171).
 - Click Edit beside a rule to [modify an existing rule](#) (see page 171).
 - Click Delete beside a rule to remove it from the policy file.
 - Click Test to test the rule set against the reference configuration.
6. Click Save.

Changes to the policy file are saved in the database.

How to Create and Edit Business Policy Rules in the CA RCM Portal

The BPR wizard simplifies creation of business process rules.

Note: When you edit an existing rule, the Edit BPR screen contains a subset of options from the wizard that are relevant to the type of rule you are editing.

Step through the screens of the wizard in the following way:

1. In the Basic Information screen, provide information that describes the scope and purpose of the rule. The following fields are not self-explanatory:

Score

A numeric value that defines the importance of a violation of this rule relative to violations of other rules in the policy.

Owner

Defines the user responsible for the rule.

Business Area/Business Process

Text fields that define the scope and purpose of the rule. These fields are descriptive and do not affect processing of the rule.

- In the logic screen, specify values for the following fields to define the underlying logic of the rule:

Type

Specifies the type of entities, links, or attributes that are examined to identify violations.

Restriction

Specifies the constraint applied to examined entities.

- In the Data screen, you define the entities that are examined. You can select individual entities, or specify attribute values to select a group of entities.

Many types of rules compare two sets of entities. In these cases the Data screen is divided into two areas, left and right, and the logic of the rule is stated in terms of these two groups.

For other types of rules you define numerical thresholds, date ranges, or text matching patterns.

- The Summary screen displays rule settings, and lets you test the rule against the reference configuration before you create the rule.

Business Process Rule Types

Most rules describe a relationship between two groups of entities. You specify the members of these groups when you create or edit a rule. These groups are identified as A and B or Left and Right in BPR editing screens. The following table describes the various rule types available and the logical operator that each rule implements.

Rule Type	Restriction	Description
Role – Role	If a configuration includes role sets A, B then the following is true:	
	Only <L> May have Reason:	Only users that have role in A (left) may have access to role in B (right).
	<L>Must have Reason:	Users in that have role A (left) must have access to role in B (right).
	<L> Forbidden to have Reason:	Users that have role in A (left) are forbidden to have access to role in B (right).
	<L> Only allowed to have Reason:	Users that have role in A (left) are only allowed to have access to role in B (right) and no other roles.
Role – Resource	If a configuration includes role set A and resource set B then the following is true:	
	Only <L> May have Reason:	Only users that have role in A (left) may have access to resource in B (right).
	<L> Must have Reason:	Users that have role in A (left) must have access to

Rule Type	Restriction	Description
		resource in B (right).
	<L> Forbidden to have Reason:	Users that have role in A (left) are forbidden to have access to resource in B (right).
	<L> Only allowed to have Reason:	Users that have role in A (left) are only allowed to have access to resource in B (right) and no other resource.
Resource – Resource	If a configuration includes	resource sets A, B then the following is true:
	Only <L> May have Reason:	Only users that have access to resource in A (left) may have access to resource in B (right).
	<L> Must have Reason:	Users that have access to resource in A (left) must have access to resource in B (right).
	<L> Forbidden to have Reason:	Users that have access to resource in A (left) are forbidden to have access to resource in B (right).
	<L> Only allowed to have Reason:	Users that have access to resource in A (left) are only allowed to have access to resource in B (right) and no other resource.
Resource – Resource (by Roles)	If a configuration includes	resource sets A, B then the following is true:
	Only <L> May have Reason:	Only users with roles that have access to resources in A (left) may have access to resources in B (right).
	<L> Must have Reason:	Users with roles that have access to resources in A (left) must have access to resources in B (right).
	<L> Forbidden to have Reason:	Users with roles that have access to resources in A (left) are forbidden to have access to resources in B (right).
	<L> Only allowed to have Reason:	Users with roles that have access to resources in A (left) are only allowed to have access to resources in B (right) and no other resource.
User Attribute - Role	If a configuration includes	User Attribute sets A, and Role B then the following is true:
	Only <L> May have Reason:	Only users with user attributes in A (left) may have access to roles in B (right).
	<L> Must have Reason:	Users with user attributes in A (left) must have access to roles in B (right).
	<L> Forbidden to have Reason:	Users with user attributes in A (left) are forbidden to have access to roles in B (right).
	<L> Only allowed to have Reason:	Users with user attributes in A (left) are only allowed to have access to roles in B (right) and not other role.
User Attribute -	If a configuration includes	User Attribute sets A, and Resource B then the following

Rule Type	Restriction	Description
Resource	is true:	
	Only <L> May have Reason:	Only users with user attributes in A (left) may have access to resources in B (right).
	<L> Must have Reason:	Users with user attributes in A (left) must have access to resources in B (right).
	<L> Forbidden to have Reason:	Users with user attributes in A (left) are forbidden to have access to resources in B (right).
	<L> Only allowed to have Reason:	Users with user attributes in A (left) are only allowed to have access to resources in B (right) and not other resource.
User Attributes Constraints	If a configuration includes	User Attributes Constraints then the following is true:
	Only <L> May have Reason:	Only users with user attribute constraint in A (left) may have access to user attribute constraint in B (right).
	<L> Must have Reason:	Users with user attributes constraint in A (left) must have access to user attributes constraint in B (right).
	<L> Forbidden to have Reason:	Users with user attributes constraint in A (left) are forbidden to have access to user attributes constraint in B (right).
	<L> Only allowed to have Reason:	Users with user attributes constraint in A (left) are only allowed to have access to user attributes constraint in B (right) and no other.
Segregation of Duty Roles	Should have no more than	The right entity must be a numeric value (N), e.g., 5. Users should have no more than N of the roles in A.
	Should have at least	The right entity must be a numeric value (N), e.g., 5. Users should have at least N of the roles in A.
	Should have exactly	The right entity must be a numeric value (N), e.g., 5. Users should have N of the roles in A.
Segregation of Duty Resources	Should have no more than	The right entity must be a numeric value (N), e.g., 5. Users should have no more than N of the resources in A.
	Should have at least	The right entity must be a numeric value (N), e.g., 5. Users should have at least N of the resources in A.
	Should have exactly	The right entity must be a numeric value (N), e.g., 5. Users should have exactly N of the resources in A.
User Counter of Roles	Should have no more than	The right entity must be a numeric value (N), e.g., 5. Roles in A should have no more than N users.
	Should have at least	The right entity must be a numeric value (N), e.g., 5. Roles in A should have at least N users.

Rule Type	Restriction	Description
	Should have exactly	The right entity must be a numeric value (N), e.g., 5. Roles in A should have exactly N users.
User Counter of Resources	Should have no more than	The right entity must be a numeric value (N), e.g., 5. Resources in A should have no more than N users.
	Should have at least	The right entity must be a numeric value (N), e.g., 5. Resources in A should have at least N users.
	Should have exactly	The right entity must be a numeric value (N), e.g., 5. Resources in A should have exactly N users.
User Attribute Value	Number <L> must be greater than Reason:	The numeric value of the User Attribute for the Left Entity must be greater than the numeric value listed in the Right Entity.
	Number <L> must be less than Reason:	The numeric value of the User Attribute for the Left Entity must be less than the numeric value listed in the Right Entity.
	Number <L> must be equal to Reason:	The numeric value of the User Attribute for the Left Entity must be equal to the numeric value listed in the Right Entity.
	Date <L> must be earlier than Reason:	The date for the User Attribute selected in the Left Entity must be earlier than the date listed in the Right Entity.
	Date <L> must be later than Reason:	The date for the User Attribute selected in the Left Entity must be later than the date listed in the Right Entity.
	<L> Must match regular expression Reason:	The value for the User Attribute selected in the Left Entity must match the value defined by the regular expression listed in the Right Entity.
	<L> Must not match regular expression Reason:	The value for the User Attribute selected in the Left Entity must not match the value defined by the regular expression listed in the Right Entity.
	<L> Should be empty	The value for the User Attribute selected in the Left Entity should be empty.
	<L> Should not be empty	The value for the User Attribute selected in the Left Entity should not be empty.

Chapter 12: Using Administration Functions

The administration menu provides a number of important processes that can be run only by administrators with the appropriate permissions.

This section contains the following topics:

- [Universe Settings](#) (see page 177)
- [Import and Export Connectors](#) (see page 194)
- [Job Scheduling](#) (see page 209)
- [Help Desk Integration](#) (see page 211)
- [The Transaction Log](#) (see page 214)
- [Cache Manipulation](#) (see page 217)
- [Repair CA RCM Configuration, User, and Resource Files](#) (see page 218)
- [Purging Data](#) (see page 219)
- [Properties Settings](#) (see page 224)
- [CA RCM Configuration Settings](#) (see page 228)
- [RACI Operations](#) (see page 229)
- [TMS Administration](#) (see page 231)
- [System Checkup](#) (see page 231)
- [How to Extract CA RCM Data](#) (see page 232)

Universe Settings

A universe consists of a set of related configuration files and related data files. Typically a universe contains the following configuration files:

- The Master configuration contains the real-world user and user privileges information.
- The Model configuration starts as an identical copy of the Master-configuration, but is updated to reflect changes in the user privileges or updates to the role hierarchy.
- A set of four RACI configurations are created by analyzing the model configuration to determine the users who are Responsible, Accountable, Consulted, and Informed for each resource in the configuration.
- The Accounts configuration files parallel the master and model configurations, and correlate user accounts defined on provisioning endpoints with users in the configuration.

In addition, you can define other configuration files that contain subsets of master/model data or newly imported data.

All configuration files in a universe share a common structure. When you define a universe you specify which fields store the unique ID, email, and other data for each user. These fields are used in CA RCM certification, analysis, and report processes. All configuration files in the universe must comply with these field designations.

Other files associated with the Universe can include:

- Audit cards generated by analysis of configurations in the universe
- An audit settings file that determines audit behavior for configuration files in the universe
- A file of pre-approved violations of business rules that are ignored in certification processes based on configurations in the universe

More information:

[CA RCM Configuration Settings](#) (see page 228)

[RACI Operations](#) (see page 229)

[Work with Universe Settings](#) (see page 178)

Work with Universe Settings

Use the following procedures to create, delete, or edit universes.

To work with universe settings

1. Click Administration, Settings, Universe settings from the CA RCM main menu.

The Universes list screen appears.

2. Do one of the following:

- To create a universe, click Add new.

The Create New Universe screen appears.

- To edit an existing universe, click Edit beside the universe you want to edit.

The Edit Universe screen appears.

The create screen and edit screen are identical. The fields of the edit screen show the current settings of the universe.

3. Edit the fields of the screen. The following fields are not self-explanatory:

Universe Name

Defines the name of the universe.

Note: You cannot change the name of an existing universe.

Master configuration name

Specifies the master configuration of the universe. All .cfg files uploaded to the database appear in the autocomplete list.

Model configuration name

Specifies the model configuration of the universe. All .cfg files uploaded to the database appear in the autocomplete list.

Important! Master and model configurations must be unique for each Universe. Do not define more than one universe that use the same master or model configuration.

Approved Audit Card

(Optional) Defines the list of pre-approved violations for the Universe.

Approved Alerts are

Specifies whether pre-approved violations are ignored (hidden) or grayed out in the audit card.

Configuration Login field

The field in configuration files of the universe that contains the user login ID (located in the users database file).

Configuration email field

The field in configuration files of the universe that contains the user email address (located in the users database file).

Configuration user manager field

The field in configuration files of the universe that contains the user manager ID (user approver).

Configuration role manager field

The field in configuration files of the universe that contains the role manager ID (role approver).

Configuration resource manager field

The field in configuration files of the universe that contains the resource manager ID (the resource approver).

Configuration resource application field

The field in configuration files of the universe that identifies the endpoint or source application of a resource.

Audit Settings file

Parameters and settings which define the audit and pattern-based checks performed on the master configuration each time it is imported.

Note: We recommend that you use the strings `_master` `_model` as part of the configuration file names.

4. Click Save.

The universe is created and appears in the Universes list.

Note: If an issue exists (for historical reasons) a message appears and you are asked if you want to auto-repair the issues in this message. Always click Yes.

5. Click Yes to auto-fix the issues listed in this error message.

The Please Wait bar appears. When the job is completed, the new universe appears in the Universes list.

More information:

[CA RCM Configuration Settings](#) (see page 228)

[Create RACI](#) (see page 229)

[Synchronize RACI](#) (see page 230)

Customize Tables for a Universe

You can customize the default layout of tables that the entity browser and role management screens use to display configuration data of the universe.

Note: These table definitions are also applied by default to campaign tickets based on this universe.

To customize tables for a universe

1. Click Administration, Settings, Universe settings from the CA RCM main menu.

The Universes list screen appears.

2. Click Edit beside the universe you want to edit.

The Edit Universe screen appears.

3. Select the Entity Browser - Display Settings tab.

This tab contains three table headers. The User, Role, and Resource headers show the layout of each entity table in the entity browser.

4. Customize the table headers:
 - a. Click Customize on a table header you want to modify.
The Customize dialog appears.
 - b. Use the arrow keys to add or remove column fields, and to order the columns.
 - c. Click the lock icon to make a column mandatory. Mandatory columns appear in red. Users can move a mandatory column, but they cannot remove it.
5. Click OK.
The entity browser displays configurations of this universe in the table formats you specified.

User Account Information

In many environments, user accounts on various provisioning endpoints define user access to resources. You can import this account information into special Accounts configuration files in the universe.

The Account configurations are based on the master and model configurations of the universe, and map users to their accounts on provisioning endpoints.

The Account configurations are created automatically when you import account information. These configuration files are named using the following convention:

```
modelconfig_Accounts.cfg  
masterconfig_Accounts.cfg
```

Note: *modelconfig* is the name of the model configuration in the universe.
masterconfig is the name of the master configuration in the universe.

When you use the entity browser to examine any configuration of a universe that contains Account configurations, the entity browser shows account information for each user.

How CA RCM Imports Account Information from CA Identity Manager Endpoints

CA RCM can import account information from CA Identity Manager endpoints. When you create a connector for CA Identity Manager, the import process identifies changed account information and updates the account configurations with the master and model configurations of the universe.

Note: Account information is retrieved only when you run an import connector from the CA RCM portal. If you run the import from CA RCM Data Management, CA RCM does not retrieve account information. For more information about the connector for CA Identity Manager, see the *Connector for CA Identity Manager Guide*.

Implicit Accounts

When a universe does not have account configurations, or a user has no accounts on external endpoints, account information is not available. CA RCM creates an implicit account to relate resources to users even when account information is not available from external endpoints.

The following system parameters control implicit accounts:

implicit.accounts.enabled

Specifies if CA RCM creates implicit accounts for users.

Valid values; True, False

Default: True

implicit.accounts.field.name

Specifies the field of user records that is used to name implicit accounts. Typically this is the loginID field.

implicit.accounts.field.name.universe

Specifies the field of user records that is used to name implicit accounts in the specified universe. This value overrides the value of the `implicit.accounts.field.name` property for the specified universe.

universe

Defines the universe that uses the field specified to name implicit accounts.

Implicit accounts have the following structure;

- The account name is taken from the field specified in the `implicit.accounts.field.name` property.
- The default mapped endpoint is taken from the Configuration resource application field specified for the universe.

Import CSV Data into an Account Configuration

You can import account information from a file of comma-separated values (CSV) into a special configuration that parallels the model configuration of the universe.

Note: Because file-based import is a one-time process, only use a CSV file for initial import or occasional administrative updates to account information. To keep account information updated, define a data connector job that imports account information from endpoints at regular intervals.

Note: You must have administrator-level rights in the CA RCM portal to perform this procedure.

To import CSV data into an account configuration

1. Prepare the data file.
2. Click Administration, Accounts from the main menu of the CA RCM portal. The Import Accounts screen appears.
3. Specify the target universe and the CSV file to import, and click Import. CA RCM copies new, unique records from the CSV file to the Account configurations. Existing information in the Account configurations is preserved.
4. (Optional) To verify imported account data, view the model configuration in the entity browser or open the account configurations in the Data Manager application

CSV File Structure

Each record of the CSV accounts data file must contain the following fields:

PersonID

Defines the user in the target universe who owns the imported account. This field has the same content and format as the PersonID field in the universe.

Endpoint

Defines the name of the provisioning endpoint that hosts the account. This field has the same content and format as the Configuration resource application field specified for the universe.

Account

Defines the account name as it exists on the provisioning endpoint.

The first line of the CSV file must be the following header:

```
personID,endpoint,account
```

Each line of the file must contain three values, separated by commas.

Example: CSV accounts data file

The following example shows a CSV file with four data records. The first two records map accounts to the same user, John Meade:

```
personID,endpoint,account
5467238,UNXMARKT,jmeade
5467238,NT-Security,john_meade
7635097,RACFTEST,marcus432
6523876,NT-Security,kim_bell
```

How to Use Data from CA Enterprise Log Manager

CA RCM can poll CA Enterprise Log Manager for usage data and display this data in certification reviews and information screens. For example, when you certify user access to a resource you can see how often the user actually accesses the resource.

You enable Interaction with CA Enterprise Log Manager per universe. CA RCM uses the account configurations of the universe and the values of the Configuration resource application field specified for the universe to identify endpoints, accounts, and resources in the CA Enterprise Log Manager database and map them to users.

Note: As part of its monitoring function, CA Enterprise Log Manager can retrieve CA RCM usage information from the CA RCM transaction log. See the *CA RCM Connector Guide* in CA Enterprise Log Manager documentation for detailed instructions.

Follow this general implementation process to import and display CA Enterprise Log Manager usage information:

1. If necessary, create monitored endpoints on CA Enterprise Log Manager corresponding to resources in CA RCM. Endpoints must record user access to the resource, because this is the event retrieved by CA RCM.

Note: for more information about creating CA Enterprise Log Manager endpoints, see CA Enterprise Log Manager documentation or open the Online Help for the CA Enterprise Log Manager endpoint creation wizard.

2. [Configure CA Enterprise Log Manager to support polling](#) (see page 186) requests from the CA RCM server.

3. From the CA RCM server, configure an ODBC data connection with CA Enterprise Log Manager. Edit the following CA RCM system properties to reflect the connection and login information.

usage.import.logmanager.odbc.host

Defines the network address of the target CA Enterprise Log Manager host in your environment.

usage.import.logmanager.odbc.port

Defines the port on the target CA Enterprise Log Manager host that accepts requests for usage information.

Default value: 5250

usage.import.logmanager.odbc.user

Defines the user name of the CA Enterprise Log Manager account that CA RCM uses to log in to CA Enterprise Log Manager.

usage.import.logmanager.odbc.password

Defines the password of the CA Enterprise Log Manager account that CA RCM uses to log in to CA Enterprise Log Manager.

usage.online.logmanager.https.port

Defines the HTTPS port on the target CA Enterprise Log Manager host that accepts web requests to view event details online.

Default value: 17002

usage.online.logmanager.https.certificate

Defines the HTTPS certificate name on the target CA Enterprise Log Manager host that authenticates web requests to view event details online.

usage.online.logmanager.https.password

Defines the password of the CA Enterprise Log Manager account that CA RCM uses to log in to CA Enterprise Log Manager.

usage.online.logmanager.eventviewer.query.id

Defines the CA Enterprise Log Manager query that CA RCM submits to view event details online.

Default value: CA_RCM

4. Enable CA Enterprise Log Manager data import for the CA RCM server. Edit the following CA RCM system properties:

usage.import.enabled

Specifies if usage data is retrieved from a CA Enterprise Log Manager host in your environment.

Valid values: True, False

Default: False

usage.online.logmanager.eventviewer.enabled

Specifies if users can open a window with a detailed CA Enterprise Log Manager usage log by clicking on the usage icon of an entity.

Valid values: True, False

Default: True

5. [Enable and configure display of CA Enterprise Log Manager usage data](#) (see page 189) for a universe.
6. [Map CA Enterprise Log Manager endpoints](#) (see page 190) to resources and accounts in the CA RCM universe.

The correct usage information is retrieved from CA Enterprise Log Manager for each resource in the universe.
7. To confirm feature setup, open a configuration of the universe in the entity browser, and verify that usage icons appear for users and resources.

More information:

[User Account Information](#) (see page 181)

Configure CA Enterprise Log Manager to Support Polling by CA RCM

To import CA Enterprise Log Manager usage data, you add CA RCM data queries to the CA Enterprise Log Manager query list, and configure a security certificate for the data connection between CA Enterprise Log Manager and CA RCM.

To configure CA Enterprise Log Manager to support polling by CA RCM

1. Import queries that let CA RCM view CA Enterprise Log Manager events online.
 - a. Log in to the CA Enterprise Log Manager portal as an administrator.
 - b. Navigate to the Queries pane (Queries and Reports, Queries).

- c. In the Query List area, click options, Import Query Definition.
- d. Specify the file RCM_Queries.xml file in the following directory of the CA RCM server:

RCM_install\Server\ELM

Note: *RCM_install* is the CA RCM installation directory.

CA Enterprise Log Manager imports the queries.

CA RCM invokes these queries to display detailed CA Enterprise Log Manager event history screens when users click monitored resources.

2. Create a security certificate for CA Enterprise Log Manager in the keystore of the CA RCM server.

- a. From the CA RCM server, browse to the CA Enterprise Log Manager server.

A security alert appears.

- b. Click View Certificate.

The Certificate popup displays information about the CA Enterprise Log Manager security certificate.

- c. Click the Details tab and click Copy to File.

The Certificate Export Wizard appears.

- d. Follow the wizard to export the certificate. In the Export Format screen of the wizard, select the Base-64 encoded X.509 (.CER) format.

The certificate is saved on the CA RCM server.

- e. Open a command prompt window and navigate to the directory that contains the exported certificate.

- f. Enter the following command:

```
"%JAVA_HOME%\bin\keytool.exe" -import -file "pathname_cer" -keystore
"%JAVA_HOME%\jre\lib\security\cacerts" -trustcacerts
```

Note: *pathname_cer* is the pathname of the exported certificate.

You are prompted for a password.

- g. Enter the following password, or the default cacerts password for your system:

changeit

The following prompt appears:

Trust this certificate?

- h. Enter y and press return

The CA Enterprise Log Manager certificate is installed in the keystore.

- i. Enter the following command:

```
"%JAVA_HOME%\bin\keytool.exe" -list -keystore  
"%JAVA_HOME%\jre\lib\security\cacerts"
```

You are prompted for a password.
 - j. Enter the following password, or the default cacerts password for your system:

```
changeit
```

A list of certificates appears.
 - k. Verify that a new certificate named mykey appears in the list.
 - l. Restart the JBoss application server service on the CA RCM server computer.
3. Register CA RCM on the CA Enterprise Log Manager server using the new certificate.
- a. Browse to the following address on the CA Enterprise Log Manager server:

```
https://ELM_host:5250/spin/calmap/products.csp
```

Note: *ELM_host* is the hostname of the CA Enterprise Log Manager server.
 - b. Log in as an administrator.
 - c. In the Registered Products pane, click Register.

The New Product Registration window appears.
 - d. Enter the name and password you specified for the new certificate and click Register.

The CA Enterprise Log Manager server recognizes the certificate and allows connection to CA RCM.

Enable and Configure Display of CA Enterprise Log Manager Data in a Universe

When you enable display of CA Enterprise Log Manager data for a universe, usage data from CA Enterprise Log Manager appears in all certification and approval tickets based on the universe. Usage data also appears when you view a configuration of the universe in the entity browser.

Note: After you perform this procedure, map endpoints between CA Enterprise Log Manager and the resources in the model configuration of the universe.

To enable and configure display of CA Enterprise Log Manager data in a universe

1. Click Administration, Settings, Universe settings from the CA RCM portal main menu.
The Universe Settings screen appears.
2. Locate the universe you want to support usage information and click Edit.
The Edit universe screen appears.
3. Click the Actual Usage tab.
4. To enable use of CA Enterprise Log Manager data, select the Enable actual usage data import for this universe option.
5. Define usage thresholds that determine the icon displayed in certification and entity screens.
Based on these thresholds, resources are flagged as "frequently used" or "rarely used" and users are flagged as "infrequent users" or "frequent users".
6. (Optional) Configure usage thresholds for a specific user or resource in CA RCM.

Map CA Enterprise Log Manager Endpoints

Usage data from CA Enterprise Log Manager must be mapped to CA RCM data structures. A monitored endpoint in CA Enterprise Log Manager can correspond to an individual resource in CA RCM.

Map endpoints in CA Enterprise Log Manager to each resource or account in the target CA RCM universe. CA Enterprise Log Manager data is then correctly associated with CA RCM resources.

Note: Perform this procedure only after you have populated the target universe with user and resource data.

To map CA Enterprise Log Manager endpoints

1. In the CA RCM portal, click Administration, Settings, Universe Settings.

The Universe Settings screen appears.

2. Select the target universe and click Edit.

The Edit screen appears.

3. Click the Entity Usage tab.

4. Click Refresh Usage Now.

CA RCM queries CA Enterprise Log Manager based on the model configuration of the universe.

- If the universe has an account configuration, it is also used to correlate CA Enterprise Log Manager data to CA RCM users.
- If the universe does not have an account configuration, CA Enterprise Log Manager data is correlated to the CA RCM implicit account of each user.

To identify endpoints in this initial query, CA RCM uses the values of the Configuration resource application field specified for the universe.

5. Click the Applications Mapping tab.

6. Map endpoints between CA Enterprise Log Manager and CA RCM.

- a. In the left pane, select a resource or account of the configuration.

- b. In the right-hand pane, select CA Enterprise Log Manager endpoints you want to map to the selected resource.

Mapped endpoints are shown in the center pane.

Repeat these steps for all endpoints in the configuration.

7. Click Finish to save settings.

Update Mapping of CA Enterprise Log Manager Endpoints

Over time, new endpoints are added to CALM data trees. Similarly, new resources are added to the configuration which represent new endpoints and external applications. Update the endpoint mapping in the universe periodically so that usage information is imported for these new resources.

Use the standard procedure to [map CA Enterprise Log Manager endpoints](#) (see page 190). In the Applications Mapping tab, click the Mapped column to sort applications in the universe, and list unmapped applications together. Map these applications to CA Enterprise Log Manager endpoints.

Pre-Approved Violations

If you want to ignore (hide) or gray out specific violations when doing compliance and pattern checks, you can add pre-approved violations within a specific universe. Pre-approved violations will appear on campaign and self service violation screens.

When adding pre-approved violations, you can provide an expiration date. Once the date expires, the violation is no longer pre-approved and behaves as a regular violation once again. You can also provide a comment to explain the reason to approve the violation.

If a pre-approved violation has an expiration date or explanation provided, both appear in the violation tooltip when you hover over the violation.

A scheduled task runs at a configurable interval, searches through all universes that have an approved audit card, and deletes all expired alerts.

Add Pre-Approved Violations

You can set violations, per universe, as pre-approved. These pre-approved violations are hidden (ignored) or grayed out in compliance and pattern check audit cards.

Note: You must have administrator-level rights in the CA RCM portal to perform this procedure.

To add pre-approved violations

1. In DNA, connect to the CA RCM server.
2. Open the audit card that contains violations you want to pre-approve.
Note: A violation must be saved to the database before you set it as pre-approved.
3. (Optional) Provide an expiration date or a comment, as follows:
 - a. Right click the violation and select Edit.
 - b. If you want to provide an expiration date, select the Expiration Date check box and provide a date.
 - c. If you want to provide a reason for the pre-approval, go to the Pre-Approve comment field and enter the text.
 - d. Click OK.
4. Right click the violation you want to pre-approve and select Always Approve this Violation.
5. Verify that the violation appears in the audit card titled *universe_name* Pre Approved Violations.

Configure Pre-Approved Violations

If you added pre-approved violations to a universe, you can specify whether the violation appears grayed out or is ignored (hidden) altogether. You configure pre-approved violations under Universe Settings.

To configure pre-approved violations

1. In the CA RCM portal, go to Administration, Settings.
2. Click Universe Settings.
3. Find the universe with the pre-approved violations to configure, and click Edit.

The Edit screen for the universe appears.

4. Next to 'Approved alerts are:', select the display configuration you want for pre-approved violations.
Default: grayed out
5. Click Save.

Configure Cleanup Task for Expired Pre-Approved Violations

In CA RCM, you can enable or disable a scheduled task to search through all universes that have an approved audit card, and delete all expired alerts. This scheduled task can be configured using the CA RCM portal.

To configure the scheduled task to clean up expired violations

1. In the CA RCM portal, go to Administration, Settings.
2. Click Property Settings.
3. Click Edit and change either of the following settings:
 - `audit.delete.expired.alerts.enabled`—enables or disables the cleanup of expired pre-approved violations
Default: True (enabled)
 - `audit.delete.expired.alerts.interval.seconds`—second interval between each cleanup
Default: 86400 (one day)
4. Click Save.

Note: If you want to override the default behavior for a specific universe, create a universe-specific property, for example, you can create the property `universe.property.Universe \ Name.audit.delete.expired.alerts.enabled` and set it appropriately for that universe. Spaces in a universe name are replaced with a backslash followed by a space (\).

By default, web services do not include pre-approved violations. If you want to include pre-approved violations, set the following property:

```
audit.approved.alerts.webservices.include=true
```

If you want to override the default behavior for a specific universe, create a universe-specific property and set it to true, as follows:

```
universe.property.My\ Universe\ Name.audit.approved.alerts.webservices.include=true
```

Note: Spaces in a universe name are replaced with a backslash followed by a space (\).

Use Case: Pre-Approved Violations

You need a few people from the Human Resources department to help the Finance department during a busy time at the end of the year.

To help out, the employees from the Human Resources department must access financial resources that would normally generate a violation within CA RCM.

Once you give the Human Resources employees access to the financial resources, you then test for compliance, and add the resulting violations to the pre-approved violations list. Finally, set the expiration date of each pre-approved violation to the first day of the next year.

Note: Be sure that you enable the scheduled job that deletes expired pre-approved violations.

All violations generated by this temporary work situation are suppressed until the end of the year. Depending on universe settings, these violations are hidden or grayed out in campaign tickets or self-service validation screens based on the universe.

Import and Export Connectors

Connectors are defined for importing and exporting user and user privileges (entities and the links between them) from corporate systems into CA RCM. At the end of an audit process, CA RCM compares the original configuration that was imported from an endpoint to the new configuration. CA RCM then applies changes that result from implementing corporate policies and regulatory compliance to the configuration variance between the original and the updated configuration. The resulting configuration is exported back to the endpoint using export connectors.

The type of connector that you are using determines where you perform the import and export. The CA RCM Portal allows you to define the following import or export connectors:

- Import Connectors
 - Custom Executable
 - CA RCM Configuration Document (CFG)
 - Generic Feed (CSV)
 - Database Configuration
 - CA Identity Manager
 - Pentaho Data Integration (PDI)
 - CA RCM Client Batch (SBT)

- Export Connectors
 - Custom Executable
 - Database Configuration
 - CA Identity Manager

Note: Connectors are defined explicitly as either an import connector or an export connector.

Some user and user privileges must be imported directly into CA RCM using the Import option in the CA RCM Data Management (DM) client tool. The Import option enables importing from the following endpoints:

- Import
 - CSV files
 - LDIF files
 - Active Directory
 - RACF
 - TSS
 - UNIX
 - SAP
 - Windows Shared Folder
 - ITIM
 - Control SA
- Export:
 - Active Directory
 - RACF
 - SQL Database
 - CSV files
 - ITIM V4.5 and V4.6
 - Control SA

Note: For more information, see the *DNA Data Management User Guide*.

Important! Some connectors exist in both the CA RCM portal and the CA RCM Data Management client tool. In these cases, we recommend running the connector located in the CA RCM portal for the following reasons:

- The job definition is saved on the portal, letting you repeat import and export tasks.
- Retrieved data is integrated directly into the universe.
- New data can be automatically synchronized with RACI definitions of the configuration.
- New user records can be automatically enriched with data from Human Resources records or other sources.

CA RCM Connectors

The following *import* connectors are available through the CA RCM portal:

Custom Executable

Allows you to write a script or executable in any language (Perl, C++, C#, Java, and so on) for importing data into CA RCM.

The executable must create 7 CSV files (Users.udb, Resources.rdb, Roles.csv, UserRole.csv, UserResource.csv, RoleRole.csv, RoleResource.csv), and CA RCM imports the information from those files.

CA RCM Configuration Document (CFG)

Reads a CA RCM file that represents a snapshot of privileges and role definitions.

Generic Feed (CSV)

Reads CSV files as input, then creates a CA RCM configuration. The CSV (Comma Separated Values) format is the most common import and export format for spreadsheets and databases. CSV files can then be manipulated and extended using simple tools such as Excel, if necessary.

The Generic Feed uses seven CSV files as input, with each individual file representing one entity type (such as users database and resources databases) or one relation between two entity types (roles). Some of the files are optional and if not specified at the time of import are assumed to be empty. The connector produces one output file, which is the CA RCM configuration file.

Database Configuration

Allows for importing information from a CA RCM configuration (in the database) into the master and model configurations.

CA Identity Manager

Integrates CA RCM with CA Identity Manager by automatically synchronizing role-based privileges between the two systems. Use the connector to import CA Identity Manager data.

Pentaho Data Integration (PDI)

Invokes Pentaho Data Integration (PDI) transformations and jobs. This feature allows for complex ETL (Extract, Transform, and Load) operations during data import. To use the PDI connector, set the *pdi.home* property to the path where PDI is located on your system.

CA RCM Client Batch (SBT)

Executes batch processing. You may need to specify dynamic parameters for file names that are defined in the SBT files.

The following *export* connectors are available through the CA RCM portal:

Custom Executable

Allows you to write a script or executable in any language (Perl, C++, C#, Java, and so on) for exporting data from CA RCM.

The executable must create a DIFF file in the CA RCM DIFF file format, and CA RCM reads the DIFF file and applies the changes.

Database Configuration

Allows for exporting information from one CA RCM model configuration to another configuration in the database.

CA Identity Manager

The connector for CA Identity Manager lets you integrate CA RCM with CA Identity Manager by automatically synchronizing role-based privileges between the two systems. Use the connector to export updated data from CA RCM to CA Identity Manager.

How to Define Connectors in the CA RCM Portal

Define import and export connectors in the CA RCM portal by using the Connector Settings screen. The Connector Settings screen provides the following two connector tables:

- Imports
- Exports

Each table displays a list of available connectors, and provides the options to Edit, Delete, Run, or Schedule a connector. The Add New button, located above each table, allows you to configure a new import or export connector.

To access the Connector Settings screen

1. Log in to the CA RCM portal as an administrator.
2. Go to Administration, Settings.
The list of available options appears.
3. Click Connector Settings.
The Connector Settings screen opens.

Define an Import Connector

CA RCM import connectors import data from endpoint systems.

Note: For more information, see the *DNA Data Management User Guide*.

To define an import connector

1. Log in to the CA RCM portal as an administrator.
2. Go to Administration, Settings.
The list of available options appears.
3. Click Connector Settings.
The Connector Settings screen opens.
4. Above the Imports table, click Add New.
The Add New Import screen appears.
5. Provide the following information for the connector:

Import client name

Defines the name for the import connector.

Description

Defines the description of the import connector, such as the connector's use, timing, and so on.

Universe

Specifies the universe that is associated with the import connector. The data obtained through this connector is imported into the universe's master configuration files. If it is an initial import and there are no pre-existing configuration files, the import process creates the configuration files.

Note: Before you can run a connector job, explicitly declare a login field for the universe and [verify that the connector maps the endpoint data to this field](#) (see page 204).

(Optional) Enrichment User Database

Defines an existing user database (.udb) file that CA RCM uses to enrich new user records during data polling. Data is imported from a specific endpoint, however, you can enrich the original data by adding additional information from a second source. For example, you can download user information from a security-related endpoint, and then enrich the data by accessing additional information from a human resources database. This data could include user addresses which were not available from the primary source of information.

Note: Enter the file name, but do not enter the .udb suffix. For example, enter **enrich** to reference the enrich.udb file.

Ticket Template

Specifies the ticket format that is used to track the job in your Inbox. Select FlowTicketforImport_V0.8.

Workflow process name

Specifies the Workpoint business process that CA RCM uses to implement the connector job. Select Import Configuration.

Max duration time

Defines an estimated processing time for the job. If the job continues beyond this time limit, CA RCM lists the job as overdue in your Inbox, but continues to process it.

Priority

Specifies the importance of the job relative to other tasks in your Inbox.

Severity

Specifies the importance of errors generated during job processing, relative to other tasks in your Inbox.

6. Select the Connector Type and provide values for all the properties that appear under Connector Information. On-screen text provides more information beside each property.
7. Click Save.

The import connector is defined and now appears in the Imports table.

More information:

[Using Tickets and the Inbox](#) (see page 23)

Enrichment User Database

During data import, CA RCM can add information to the empty fields of new user records. For example, human resources data or other organizational information is used to enrich new user records.

The enrichment values are drawn from an existing user database. To implement data enrichment, specify the database when you define the connector job. The data in this enrichment database overwrites any imported field values.

The following CA RCM system properties control this feature.

hr.enrichment.clear_empty

Specifies how empty fields in the enrichment database affect imported data.

True

Omits values during data import when the corresponding field in the enrichment database is empty.

False

Writes imported values to the target CA RCM configuration when the corresponding field in the enrichment database is empty.

hr.enrichment.clear_missing

Specifies how missing fields in the enrichment database affect imported data.

True

Omits values during data import when the corresponding field in the enrichment database is missing.

False

Writes imported values to the target CA RCM configuration when the corresponding field in the enrichment database is missing.

Automatic RACI Synchronization

The CA RCM server uses [RACI subconfigurations](#) (see page 229) to control end-user access to CA RCM portal functions. When you import new user records into a configuration, you can automatically enroll these new users in that configuration's RACI hierarchy.

If an imported user does not have a login name (LoginID field is blank), they cannot access the CA RCM portal. The automatic RACI synchronization process flags these users, and notifies the portal administrator.

Define an Export Connector

CA RCM export connectors export data to endpoint systems.

Note: For more information, see the *DNA Data Management User Guide*.

To define an export connector

1. Log in to the CA RCM portal as an administrator.
2. Go to Administration, Settings.
The list of available options appears.
3. Click Connector Settings.
The Connector Settings screen opens.
4. Above the Exports table, click Add New.
The Add New Export screen appears.
5. Provide the following information for the connector:

Export client name

Defines the name for the export connector.

Description

Defines the description of the export connector, such as the connectors use, timing, and so on.

Universe

Specifies the universe to be associated with the connector.

Note: Before you can run a connector job, explicitly declare a login field for the universe and verify that the connector maps the endpoint data to this field.

Ticket Template

Specifies the ticket format that is used to track the job in your Inbox. Select FlowTicketforExport_V0.4.

Workflow process name

Specifies the Workpoint business process that CA RCM uses to implement the connector job. Select one of the following:

- Export Master Model Deltas
- Export Master Model Deltas with model auto fix—creates an audit card that contains all the new roles that need to be created in order to fix the model. Use with CA Identity Manager connector only.
- Export Master Model Deltas with model fix—creates an error ticket with links to the audit card, when errors are found in the model. Use with CA Identity Manager connector only.

Max duration time

Defines an estimated processing time for the job. If the job continues beyond this time limit, CA RCM lists the job as overdue in your Inbox, but continues to process it.

Priority

Specifies the importance of the job relative to other tasks in your Inbox.

Severity

Specifies the importance of errors generated during job processing, relative to other tasks in your Inbox.

6. Select the Connector Type and provide values for all the properties that appear under Connector Information. On-screen text provides more information beside each property.
7. Click Save.

The export connector is defined and now appears in the Exports table.

Export to CA Identity Manager AutoFix

The export process to CA Identity Manager has been enhanced to automatically fix any errors in the model configuration. When creating a CA Identity Manager connector, you can select one of the following new [workflow processes](#) (see page 198):

- Export Master Model Deltas with model auto fix—creates an audit card that contains all the new roles to create to fix the model
- Export Master Model Deltas with model fix—if errors were found in the model, creates an error ticket with links to the audit card.

If you select one of the previous workflow processes, the following logic is applied to CA RCM data before exporting it into CA Identity Manager:

- When connecting a resource to a provisioning role, the resource is linked to the account template belonging to the same provisioning role on the endpoint where the account template resides. If there is no such account template, CA RCM creates it.
- When connecting a parent account template to a child provisioning role, the link direction is inverted.

- When creating a CA RCM role, the type is set as follows:
 - If the role type is "Role" or "Provisioning Role", it is exported as a provisioning role.

The role type is set to the default value of the connector.

If the role has directly linked resources, they are moved to the linked account templates, as mentioned previously.
 - If the role type is "Policy", "Provisioning Policy", or "Account Template", it is exported as an account template.

The role type is set to the default value of the connector.
- If the role does not start with a valid endpoint type, the creation fails with a detailed message.
- If the role has directly linked users, the addition fails with a detailed message.
- If the role has resources that are not of the relevant endpoint type, the addition fails with a detailed message.
- If a role has no type, it is exported as a provisioning role. All details for this export are as previously described.

Run or Schedule a Connector Job

You can run predefined connector jobs that exchange data with external systems.

To run or schedule a connector job

1. [Declare a login field for the universe](#) (see page 204), and verify that the connector maps endpoint data to this field.
2. In the CA RCM portal, go to Administration, Settings, and click Connector Settings.

The Connector Settings screen appears.

3. Do *one* of the following:
 - Click Run adjacent to the connector job you want to run. The connector job begins immediately.
 - Schedule the future execution of a connector job, as follows:
 - a. Click Schedule.

The New Connector Scheduled Task dialog appears.

- b. Complete the following fields:
 - First execution—Specifies the date and time at which the job is first run.
 - Number of additional repeats—Defines the number of times you want to run the job. Enter the value -1 to define an unending series.
 - Repeat interval—Defines the time period between executions in the series.
- a. Click OK

The schedule is saved and the connector job runs at the scheduled times.

Verify Mapping of the Login Field

When CA RCM creates new user records based on endpoint data, it automatically creates accounts for these users in the CA RCM portal. To support this, the connector job must map a valid value to the login field of the target universe.

To verify mapping of the login field

1. Verify that the target universe has a defined login field, as follows:
 - a. In the CA RCM portal, go to Administration, Settings, and click Universe Settings.

The Universe settings screen appears.
 - b. Locate the universe you specified for the connector job, and click Edit.

The Edit screen appears.
 - c. Verify that the Configuration login field refers to an existing field in the Universe. If the Configuration login field is empty, define it by selecting a field.
 - d. Note the name of the Configuration login field.
2. Verify that the connector maps data to the login field, as follows:
 - a. Open the mapping XML file you specified for the connector job.
 - b. Locate the line that maps the Login field. The line contains the following term:

```
host='Login'
```
 - c. Verify that endpoint data is mapped to this field in the **guest** term. If this mapping is empty, define it by specifying an endpoint data field.

More information:

[Universe Settings](#) (see page 177)

Import and Export Tickets

When an import or export operation fails, the CA RCM portal generates an Error Ticket.

The Error ticket provides the following functionality:

Close

Closes the ticket.

Save

Saves any changes made to the ticket.

Delegate

Transfers the ticket to another manager.

Escalate

Transfers the ticket to another manager.

Acknowledge

Disabled until the process is completed. Click this button to complete and archive the ticket.

Handle

Verifies that if multiple users received this error ticket, only one will handle it. After one user clicks this button, the functional buttons for this ticket will be disabled in the other users' ticket.

Terminate job

Manually terminates the currently running job.

(CA Identity Manager Export only) Fix (see page 202)

Fixes the job and continues with the export.

Clean up

Cleans up the temp files prior to terminating the job.

How to Define and Run a Multi-Import Job

You can use the multi-import feature to group several import jobs that update a single universe. The result is a single job that imports data from several sources and merges them into one configuration file.

The following two steps implement a multi-import job:

1. [Define a multi-import job](#) (see page 206) and each of its connectors in the CA RCM portal.
2. [Run or schedule](#) (see page 203) this multi-import job using the job scheduling tools of the CA RCM portal.

When the multi-import job merges data from several sources, it reconciles the data mappings of the various sources. The resulting configuration file may not match the data scheme of existing configurations in the universe. Note the following:

- If you [use a multi-import job to populate a new, empty universe](#) (see page 207), the merged configuration defines the default data scheme of the universe. This example is the most common use of multi-import.
- If you use multi-import to import data into an existing universe, verify that all the data sources have data mappings that match each other and the universe.

Define a Multi-Import Job

You can define a multi-import job in the CA RCM portal. Run this job to import data from several sources automatically.

Note the following:

- When using multiple configuration files as data sources, all the files must have the same schema as the target universe, for example, all files must use the same field for PersonID, the same field for email, and so on.
- Multi-import does not correlate imported user information from several data sources. To identify likely matches, overlap, and duplicates between multiple data sources, see the UUID documentation in the *Data Management User Guide*.

To define a multi-import job

1. Log in to the CA RCM portal as an administrator.
2. Go to Administration, Settings, and click Multi Import.

The Multi Import main screen appears.

3. Click Add New.

The Multi Import editing screen appears.

4. Enter values for the Name and Description fields of the multi-import job.
5. Specify the Universe to update from the Universe drop-down list.
6. Add an import task to the multi-import job, as follows:
 - a. Select the type of import job you want from the Select Connector Import Implementation drop-down list.
 - b. Click Configure & Add To Merge.

A configuration screen appears. Fields for the type of import job you selected are listed.
 - c. Provide values for all connector properties that appear.
 - d. Click Done.

The new import task appears in the table.
7. Repeat Step 6 to define as many import tasks as you need.
8. (Optional) Click Delete in the row of an import task you want to remove.
9. Set the completion level for the job as follows:
 - a. Click the Manage Groups link at the top right of the screen.

The Manage Group window appears.
 - b. Click Edit to edit the default group.

The Group window appears.
 - c. Edit the Completion Level field.

Note: This field defines the percentage of import tasks that must complete successfully for the multi-import job to be successful. For example, if a multi-import job contains 20 tasks, and its Completion Level is set to 75, then the job is successful if 15 of those tasks complete successfully ($15/20=75$ percent). **Default:** 100
 - d. Click Save twice.

The completion level is set for the job.
10. In the Multi Import editing screen, click Save.

The Multi Imports main screen appears. The new multi-import job is listed in the table.

Use a Multi-Import Job to Populate an Empty Universe

A multi-import job enables you to build a new universe with CA RCM data. You can define and run a single job that automates the following processes:

- Data import from several provisioning nodes or other sources
- Reconciliation of field mapping across data sources

- Data merges from various import connectors
- Configuration generation with a best-fit data scheme
- Universe population with imported data

The multi-import process expects to find a master and model configuration in the target universe. When you run a multi-import job based on an empty universe, you use the process ticket in the Inbox to create the master and model configuration files.

To use a multi-import job to populate an empty universe

1. [Define a new universe](#) (see page 178) in the CA RCM portal. Specify dummy names for the master and model configurations. Do not use names of existing configurations.
2. [Define a multi-import job](#) (see page 206). Select the universe defined in Step 1.
3. [Run the job](#) (see page 203).
4. Click Inbox on the CA RCM portal main menu.
Your Inbox appears, containing a Multi Import ticket and an Error Handling ticket for the multi-import job.
5. Double-click the Error Handling ticket.
A Ticket Properties Form dialog opens.
6. Open the More section of the form. The following message appears:
Results for checking if database contains master and model configuration as defined in universe [universe_name]: The master configuration [master_name] Does not exist in the database, The model configuration [model_name] Does not exist in the database
Note: *universe_name*, *master_name*, and *model_name* are the names you specified when you defined the new universe.
7. Click Handle.
The Create Universe button appears.
8. Click Create Universe.
The error is resolved.
9. Return to the Inbox and click Refresh.
The queue lists a new Error Handling ticket.
10. Double-click the Error Handling ticket.
A Ticket Properties Form dialog opens.

11. Open the More section of the form. The following message appears:

Failed to compare the universe master configuration with the Permissions configuration. The universe [universe_name] does not have "LoginID" field mapping, please go to Administration > Settings > Universe Settings and map the "LoginID" field.

12. Click Handle.

The Skip Synchronization button appears.

13. Click Skip Synchronization.

The error is resolved. The Multi Import job proceeds.

Note: You can open the Multi Import ticket to monitor the progress of the job.

Job Scheduling

Job Scheduling enables you to set up automatic and repeated CA RCM jobs. Each job is assigned to a universe and an appropriate ticket is sent to the administrator's Inbox when the job is completed.

To access Job Scheduling information, go to Administration, and click Job Scheduler. This brings up the Jobs table.

Run or Schedule a Job on the CA RCM Portal

You can run predefined connector jobs or other processes in the CA RCM portal.

To run or schedule a job in the CA RCM portal

1. Locate the job or process you want to run.
2. Do *one* of the following:
 - Run the job immediately by clicking Run in the row of that process.
The job begins immediately.
 - Schedule one or more future jobs, as follows:
 - a. Click Schedule in the row of that process.
The Schedule Task dialog appears.

b. Complete the following fields:

- First execution—Defines the date and time at which the first job is initiated
- Additional repeats—Defines the number of job instances you want to generate. Enter the value -1 to define an unending series of jobs.
- Repeat interval—Defines the time period between jobs in the series.

a. Click OK.

The schedule is saved. CA RCM automatically initiates the jobs according to the schedule.

The Jobs Table

The Jobs table lists all the jobs that have been entered into the system. The table contains the following fields:

Job Name

Defines the name of the job.

Description

Provides a description of what the job does.

Job Class

Lists the Java Class of the job.

Start Time

Provides the date and time on which the job will begin.

Previous Execution

When a job repeats, defines the previous date and time it ran is listed here.

Next Execution

Defines the date and time when the job is scheduled to repeat.

Delete

Allows you to delete the job.

Help Desk Integration

CA RCM can be configured to integrate with other help desk systems, such as CA Service Desk Manager. In this release, the help desk integration is limited to viewing information in the CA RCM ticket. Once you configure integration, you are able to view this information within a help desk ticket.

Note: No custom CA RCM properties or operations are currently provided with this integration.

To configure help desk integration within CA RCM, perform the following process.

1. Set help desk integration properties within CA RCM.
2. Import help desk user information into CA RCM.

Set Properties for Help Desk Integration

To set up Help Desk integration, set basic and ticket type mapping properties within the CA RCM portal.

To set properties for help desk integration

1. In the CA RCM portal, go to Administration, Settings.
2. Click Property Settings.

The Properties screen appears.

3. Click Add New (or Edit, if the property exists) and set the following properties:

tmsEvent.create.enable

Defines whether to delegate CA RCM ticket creation events to clients, such as a help desk application.

Values: True/False

integration.unicenter.servicedesk.username

Defines the help desk user name used to access CA RCM, such as administrator.

integration.unicenter.servicedesk.password

Defines the password for the help desk user.

integration.unicenter.servicedesk.webservice.url

Defines the help desk Web Service URL.

Note: CA Help Desk r12 exposes a new Web Service, but CA RCM only supports the r11 Web Service.

integration.unicenter.servicedesk.user.field

Defines the field in the permission configuration user database (eurekify.udb) that states the login ID of the user in the help desk system.

Note: If not specified, PersonID is used.

integration.unicenter.servicedesk.type.mapping

Defines the mapping between RCM ticket types and the help desk ticket types, using a key value pair.

Example: TMS:TestTicket=*ChangeOrder*,SAGE:*RoleTicket=Bug, SAGE:ErrTicket=Issue

The previous example details the following:

- Maps the CA RCM test ticket to the help desk *ChangeOrder*
- Maps the CA RCM error ticket to the help desk 'Issue' ticket
- Maps any CA RCM ticket with a type that ends in 'RoleTicket' to a help desk ticket of 'Bug' type. (SAGE:*RoleTicket=Bug)

integration.unicenter.servicedesk.object.type.ChangeOrder

Defines the help desk object type of the *ChangeOrder* ticket.

integration.unicenter.servicedesk.attributes.ChangeOrder

Defines attributes of the *ChangeOrder* ticket. Use the velocity template language to set the values for this property. [Predefined variables](#) (see page 212) are available to set these values.

Examples:

```
chg_ref_num, RCM_1_${ticket.getTicketId()}_${currentTime},
description, ${ticket.getDescription()},
summary, ${ticket.getTitle()},
affected_contact, ${ticketOwnerHandle},
requestor, ${loginUserHandle} =
```

Note: For more information about the velocity template language, see <http://velocity.apache.org/engine/releases/velocity-1.6.2/user-guide.html>.

Predefined Variables

The following variables can be used to populate help desk ticket attributes. These variables are used in setting the integration.unicenter.servicedesk.attributes.*ChangeOrder* property.

- sid—the result of the service.login() method
- ticket—the ticket VO instance. See the TicketVO class documentation in the open API.

- `service`—the web service instance, generated from `http://some_server:8080/axis/services/USD_WebServiceSoap?wsdl`
- `ticketOwnerHandle`—the handle returned by the `service.getHandleForUserid()` method of the user the ticket relates to
- `loginUserHandle`—the handle returned by the `service.getHandleForUserid()` method of the user specified at `"integration.unicenter.servicedesk.username"`
- `currentTime`—`System.currentTimeMillis()`;
- `currentDateObject`—`java.util.Date` representation of `System.currentTimeMillis`
- `currentTimeFormatted`—`SimpleDateFormat.getTimeInstance().format(currentDateObject)`
- `currentDateFormatted`—`SimpleDateFormat.getDateInstance().format(currentDateObject)`
- `ticketLinkHtml`—an html link element (`Action:`) with a reference to the CA RCM ticket
- `ticketQueueUrl`—the value of the `portalExternalLink.ticketQueueUrl` property. For example, `http://localhost:8080/eurekify/`

Import Help Desk User Information to the `eurekify.udb`

To complete help desk integration, set the permission configuration of the help desk user in the CA RCM user database (`eurekify.udb`).

To import help desk user information

1. In CA RCM Data Management, go to File, Open from Database.
2. In the Choose File Type drop-down list, select User Database Files.
3. Select `Eurekify_Users.udb` and click Next.
4. Go to File, Save to File as, and save the `Eurekify_Users.udb` as a file.
5. Edit the saved file and add the help desk account name information as an additional field.

6. In CA RCM Data Management, go to Management, Merge User Database and merge the saved file into the database, as follows:
 - a. In the Files dialog, enter the following values:
 - First Users DB: the path to the saved database file that you edited in Step 5.
 - Second Users DB: the path to the original CA RCM database
 - Output Users DB: the path to the output CA RCM database
 - b. Click Merge.

The Transaction Log

The CA RCM Transaction Log (TxLog) provides detailed information about actions taken in the CA RCM server. The transaction log also records all changes to user, role, and resource entities.

Note: the transaction log records entity changes only for the data files you specify. For more information, see the *Data Management User Guide* or the *DNA User Guide* for this release of CA RCM.

A table summarizing transaction log entries is located in the Developer Resource folder of the **CA-RCM-rel#-Language-Files.zip** file of the CA RCM installation package.

When you first open the Transaction Log page, the table is empty and you can see a filter that you can use to select which transactions you want to view. The entries are listed by date.

<Column>

Select the column that will determine which transactions will be viewed in the Transaction Log table. You can filter the table contents based on the following options:

- Source: The subsystem where the transaction originated.
- Owner: Owner or ticket ID
- SData1
- SData2
- SData3

<text box>

Enter any data that may appear in the selected column to further filter the transactions. The text is case sensitive.

OK

Updates the data presented in the transaction log table. If no filter was supplied, all the existing transactions are listed.

Delete All

Deletes all the transactions saved by the CA RCM system.

Records per page

Select the number of records that will appear in the table.

To view transactions in the Transaction Log table

1. From the portal main menu, click Administration, Transaction Log.
The Transaction Log screen opens.
2. (Optional) Filter the data you want to view in the Transaction Log table:
Select a field from the Column drop-down box and enter the field content.
3. Click OK.
The requested transaction logs appear in the Transaction Log table.
4. (Optional) Click Delete All to delete all the transactions currently saved by the system.

Track Portal Usage in the Transaction Log

The CA RCM server records user actions and changes to entities in its transaction log file. You can track user interaction with the CA RCM portal in the transaction log.

Note: You must have administrator-level rights in the CA RCM portal to perform this procedure.

To track portal usage in the transaction log

1. From the main menu, click Administration, Settings, Properties Settings.
The Properties Settings window appears.
2. Modify the following CA RCM system properties to enable and configure tracking of portal usage.

Note: To see all system properties that control transaction log tracking, filter the properties list using the string **txlog**.

txlog.portal.login.enable

Specifies whether to record an event in the transaction log when a user logs in to the CA RCM portal.

Values: True, False

txlog.portal.logout.enable

Specifies whether to record an event in the transaction log when a user logs out of the CA RCM portal.

Values: True, False

txlog.webservice.login.enable

Specifies whether to record an event in the transaction log when a web service logs in to the CA RCM portal.

Values: True, False

txlog.portal.pageaccess.enable

Specifies whether to record events in the transaction log when users navigate in the CA RCM portal.

Values: True, False

txlog.portal.pageaccess.include.pageclasses

Specifies the pages of the portal to include when tracking user navigation in the CA RCM portal. Identify pages of the portal by their class names, and format the list as comma-separated values.

Example: The following string enables tracking of user navigation to the portal homepage and the top-level dashboard and entity browser pages:

```
com.eurekify.web.portal.homepage.HomePage,com.eurekify.web.dashboards.ConfigurationDashboardPage,com.eurekify.web.entitybrowser.EurekifyBrowserPage
```

txlog.portal.pageaccess.exclude.pageclasses

Specifies the pages of the portal to exclude when tracking user navigation in the CA RCM portal. Identify pages of the portal by their class names, and format the list as comma-separated values.

Default: com.eurekify.web.portal.EmptyPage

3. Save changes to system properties.

Interactions with the CA RCM portal are recorded in the transaction log as defined.

More information:

[Editing a Property Key](#) (see page 227)

Cache Manipulation

Using the CA RCM server's cache improves performance. This is achieved by uploading the current Universe and configuration data to the cache. Accessing the server's cache is much faster than accessing the hard drives, so users can receive information more quickly than if they had to receive content from the server hard drives.

This section covers the following topics:

- Loading the cache
- Clearing the cache

More information:

[Load Cache](#) (see page 218)

[Clear the Cache](#) (see page 218)

Load Cache

This utility is used to swiftly load a specific configuration into the CA RCM Server's memory cache.

To load a specific configuration into the CA RCM Server's memory cache

1. On the Administration menu click Cache and then select Load Cache.
The Load Cache screen opens.
2. Select a Configuration from the drop down list and click OK.

Clear the Cache

This utility is used to swiftly clear the CA RCM Server's memory cache. It is useful in the special case where you updated the configuration data (for example changing permissions) in the DNA and you want to make sure that anyone running the system will use the updated data.

To clear the cache

1. On the Administration menu click Clear Cache.
The Clear Cache screen opens.
2. Click Clear Caches to clear the CA RCM Server's memory cache.

Repair CA RCM Configuration, User, and Resource Files

Editing and data enrichment may, rarely, introduce inconsistencies in user, resource, or configuration files. You can analyze a configuration and its related user and resource data files, and correct any inconsistencies that you find. If you cannot open a user (.udb) resource (.rdb), or configuration (.cfg) file, analyze it for errors using this procedure.

Note: You must have administrator-level rights in the CA RCM portal to perform this procedure.

To repair CA RCM configuration, user, and resource files

1. Click Administration, Settings, Fix Configuration in the CA RCM portal.
The Fix Configuration screen appears.

2. Select a configuration file and click Analyze.

CA RCM analyzes the configuration file and its related user and resource files. It identifies the following errors:

- Orphaned users or resources—The configuration file lists a user or resource that is not in the source user (.udb) or resource (.rdb) file.
- Broken links—A link references a user, resource, or role that no longer exists in the configuration.
- Non-sequential user or resource file—Each record in user and resource files is assigned an internal ID number. If these internal ID numbers are not consecutive, CA RCM cannot open the file.

3. Do any of the following:

- If analysis found orphaned users, orphaned resources, or broken links in the configuration, click Fix Configuration.

Orphaned entities and their related links are removed. Broken links are also removed.

- If analysis found a non-sequential user file, click Fix UDB.

The user (.udb) file is renumbered. In addition, *all* configurations that reference this user file are cleansed of orphaned users and broken user links. Then the user list and user links of all these configurations are revised with the new internal ID numbers.

Note: This function affects other configurations in addition to the configuration you analyzed. Examine related configurations and verify their content before you run this function.

- If analysis found a non-sequential resource file, click Fix RDB.

The resource (.rdb) file is renumbered. In addition, *all* configurations that reference this resource file are cleansed of orphaned resources and broken resource links. Then the resource list and resource links of all these configurations are revised with the new internal ID numbers.

Note: This function affects other configurations in addition to the configuration you analyzed. Examine related configurations and verify their content before you run this function.

Purging Data

Good management practice requires you to purge old, unneeded data files from the CA RCM database server periodically. The purge utility simplifies this maintenance task.

Important! Purging removes data completely and permanently from CA RCM databases. Back up all data before you purge, and verify that the data you purge is not needed.

The purge utility offers three ways to purge data:

- Purge selected documents and data files.
- Purge by date—Clear the ticket database or system logs of entries older than a date you specify.
- Purge inactive portal users—Remove users of the CA RCM portal who are not associated with any current universes.

Purge Selected Documents

You can use the CA RCM portal purge utility to delete outdated or unneeded data files from the CA RCM database.

Important! Purging removes data completely and permanently from CA RCM databases. Back up all data before you purge, and verify that the data you purge is not needed.

When you purge a universe or configuration file, the following associated files are also purged:

- Related configuration files such as master, model, and RACI configurations.
- Audit Cards
- Campaigns
- Log Entries

Note: You must have administrator-level rights in the CA RCM portal to perform this procedure.

To purge selected documents

1. Click Administration, Settings, Purge Data from the CA RCM portal main menu.

The Purge Data screen appears.

2. Select the By Document option in the Purge Type drop-down, and click Next.
3. Select the type of document you want to purge in the Document Type drop-down.

The Select Values screen appears. All existing data files of the type you specified are listed.

4. Select all the documents you want to purge.

Note: Press Shift or drag your mouse to select a section of the list, or press Ctrl and click to select individual files from the list.

5. Click Next.

The Confirmation screen appears.

6. Review the scope of the data purge:

- In the Document Types area, expand the tree to see which data files are selected for purge. This list includes files based on, or derived from, the files you selected.
- In the Counters area, verify the scope of related log and ticket data that is selected for purge.

If the scope you specified includes data that you do not want to purge, do one of the following:

- Click Back to redefine the selection criteria.
- Click Cancel to abort the purge, then copy or back up needed data.

7. Click Purge.

The specified data is permanently deleted from the CA RCM database. When the purge is complete, a confirmation message appears in the Purge Data screen.

Purge Data by Date

You can use the purge utility to delete workflow tickets, transaction (Tx) log entries, or portal usage tracing data that is older than a date that you specify.

Important! Purging removes data completely and permanently from CA RCM databases. Back up all data before you purge, and verify that the data you purge is not needed.

Note: You must have administrator-level rights in the CA RCM portal to perform this procedure.

To purge data by date

1. Click Administration, Settings, Purge Data from the CA RCM portal main menu.

The Purge Data screen appears.

2. Select the By Date option in the Purge Type drop-down and click Next.

3. Select the type of data you want to purge in the Select Type drop-down, and click Next.

The Select Values screen appears.

4. Complete the following field to define the scope of the purge;

Older Than

Defines the date of the oldest entry to retain. Entries older than this date are purged.

5. (Optional for Tx Log purge only) Filter transaction log entries using the following additional fields:

Owner

Defines the UserID or TicketID of the initiating user or ticket.

Source

Defines the CA RCM subsystem that generated the log entry.

sdata1, sdata2

Defines values in string data fields of log entries.

6. Click Next.

The Confirmation screen appears.

7. Review the scope of the data purge.

If the scope you specified includes data that you do not want to purge, do one of the following:

- Click Back to redefine the selection criteria.
- Click Cancel to abort the purge, then copy or back up needed data.

8. Click Purge.

The specified data is permanently deleted from the CA RCM database. When the purge is complete, a confirmation message appears in the Purge Data screen.

Purge Portal Users from the Permissions Configuration

Users at various levels in the enterprise access the CA RCM portal to participate in review and certification campaigns, and to use self-service role management tools. Each user must have a user account on the portal. CA RCM can create these user accounts created automatically based on retrieved user data. The *permissions configuration* file stores the portal user account information.

To preserve data integrity and the security of the CA RCM portal, periodically remove users who no longer need this access.

The purge utility automatically identifies portal users who are not affiliated with a currently existing universe. These users cannot participate in any CA RCM processes, and are candidates for deletion.

Important! Purging removes data completely and permanently from CA RCM databases. Back up all data before you purge, and verify that the data you purge is not needed.

Note: You must have administrator-level rights in the CA RCM portal to perform this procedure.

To purge portal users from the permissions configuration

1. Click Administration, Settings, Purge Data from the CA RCM portal main menu.

The Purge Data screen appears.

2. Select the Permissions Configuration User option in the Purge Type drop-down and click Next.

The CA RCM server compares portal permissions data with universe files in the database. Any portal users who are not affiliated with a universe are listed as purge candidates. If purge candidates are discovered, proceed with the purge process.

3. Select the users that you want to purge, or click the column header check box to select all users.
4. Click Next.

The Confirmation screen appears.

5. Review the scope of the data purge.

If the scope you specified includes data that you do not want to purge, do one of the following:

- Click Back to redefine the selection criteria.
- Click Cancel to abort the purge, then copy or back up needed data.

6. Click Purge.

The specified data is permanently deleted from the CA RCM database. When the purge is complete, a confirmation message appears in the Purge Data screen.

Properties Settings

The Properties Settings utility gives you access to the system property file CA RCM.properties, allowing you to create new property keys and access and edit the values of existing property keys.

For ease of use, properties that are considered to be common properties, such as of the type properties.headers.commonProperties are listed separately under the Settings sub-menu as Common Properties Settings. This utility functions in the same way as the general Properties Settings utility.

The Properties table contains the following columns:

Type

The name of the associated property file.

Property Key

The name of the property key.

Property Value

The value assigned to the property key.

The CA RCM Properties page provides the following functions:

Create New

Use to create new Property Keys.

Edit

Use to edit existing Property Keys.

Apply Filter

Use to filter the properties list.

Records per page

Select the number of records that will appear in the table.

When creating a new key or editing a new one, the data is not saved directly to the eurekify.properties file. Instead the updated property key value is saved to the CA RCM's database. When you run the CA RCM Portal, the CA RCM server checks the database property listings. If the value of a property key in the database is different than the value listed in the eurekify.properties, the system will use the value listed in the database.

Note: The database values do not change during system updates.

The CA RCM Portal provides you with two databases to store your update key values:

DB_dynamic_properties

The change is immediate. You do not have to wait for the server to go offline to update the property values.

DB_static_properties

The change will take place the next time that the server is restarted.

Note: Servers go offline for regular maintenance and backup. The changes made to the property values designated DB_static_properties will be implemented the next time the server goes back online.

To access the Properties page

1. On the Administration menu click Settings.
The list of available options appears.
2. Click Properties Settings.
The CA RCM Properties Page screen opens.

More information:

[Access the Common Properties Settings Page](#) (see page 225)
[CA RCM Properties](#) (see page 259)

Access the Common Properties Settings Page

Common properties are properties of the type `properties.headers.commonProperties`.

For instructions on how to create a new property key or edit an existing one see:

- Create a new Property key
- Edit an existing property key

To access the Common Properties Settings page

1. On the Administration menu, click Settings.
The list of available options appears.
2. Click Common Properties Settings.
The Common Properties Settings page appears.

More information:

[Creating a New Property Key](#) (see page 226)

[Editing a Property Key](#) (see page 227)

Creating a New Property Key

Property keys are defined and provided as part of the CA RCM product, out-of-the-box. At times, you may find it necessary to add a new property key to the CA RCM property file. The Properties Settings utility makes this easy to do.

When you want to create a new property key, you have to enter the key before you click Create New. If you do not, you will receive the following message: cannot create a property with a null/empty key. [GENPRP003]

After you enter the new property key name and click Create New, the Edit Property screen opens.

Save is disabled. The reason is that, for security reasons, when you edit a property key, the change is not saved directly to the properties file. Instead the updated property key value is saved to the CA RCM database.

The CA RCM Portal provides you with two databases to store your update key values:

DB_dynamic_properties

The change is immediate. You do not have to wait for the server to go offline to update the property values.

DB_static_properties

The change will take place the next time that the server is restarted.

To create a new property key

1. In the CA RCM Properties page enter a name of a property key in the text box under Properties.
2. Click Create New.
The Edit Property screen opens.
3. Enter a Property Value in the text box.
4. Select a database Type from the drop-down list.
5. Click Save. The new property appears in the Properties .

Editing a Property Key

Following system changes you may need to update the value of a property key. For example, if you change the name of the SMTP (email) server, used by your corporation to send out emails.

When you click Edit next to an existing property key, the Edit Property screen opens:

When editing an existing property, the source of the property is listed in the Type drop-down.

Save is disabled. The reason is that, for security reasons, when you edit a property key, the change is not saved directly to the properties file. Instead the updated property key value is saved to the CA RCM database.

The CA RCM Portal provides you with two databases to store your update key values:

DB_dynamic_properties

The change is immediate. You do not have to wait for the server to go offline to update the property values.

DB_static_properties

The change will take place the next time that the server is restarted.

To edit a property key

1. (Optional) In the CA RCM Properties page enter a name of a property key, or part of one, in the filter text box located below the Properties table. Click Apply Filter.

The Properties table presents only keys that match your filter criteria.

2. Click Edit next to the property key that you want to change.

The Edit Property screen opens.

3. Enter a Property Value in the text box.
4. Select a database Type from the drop-down list.
5. Click Save.

The updated property appears in the Properties screen table.

CA RCM Configuration Settings

The CA RCM permissions configuration handles user access to the CA RCM Portal. A user has access to the CA RCM Portal only if they are listed in the permissions configuration (eurekify.cfg), which is actually the configuration of internal CA RCM permissions.

When you add a new Universe to the system, prior to updating the RACI configurations, you have to make sure that all the users associated with the Universe (via the configuration) have access to the CA RCM Portal. This is necessary since the users listed in the universe's configuration may need to access the portal to perform self-service tasks (users), or approval tasks (managers), or certifications tasks (managers).

This process is also important when new users have been added to the universe's configuration.

As all persons in an organization probably already have accounts on the organization's main authorization authorities (such as, for example, Active-Directory), the best way to update the permissions configuration is from this source, which actually is one (or more) of the end-points already imported to CA RCM and residing as a configuration/universe within its database.

To check the CA RCM configuration for new users when creating a new Universe

1. On the Administration menu click Permissions Configuration Settings.
2. Click Update Permissions configuration with universe users.

The Update Permissions Configuration with Universe Users screen opens.

3. Select a Universe from the drop-down list.
4. Click Select.

An appropriate notice appears when the process is completed. For example:

5. If the system identified records that need to be updated or fixed, check the system suggestions and act as necessary.

Note: We recommend that you use the CA RCM DNA application to fix the records.

RACI Operations

The RACI model is a tool that can be used for identifying roles and responsibilities during an organizational audit, thereby making the audit process easier and smoother. The model describes what should be done by whom during audits and when corporate changes take place.

RACI is an abbreviation for:

R = Responsible, who owns the problem/project.

A = Accountable, to whom R is accountable, who must sign off (Approver) on work before it is accepted.

C = Consulted, who is to be consulted, who has information and/or the capability necessary to aid in completing the work.

I = Informed, who must be notified of results (but does not need to be consulted).

The CA RCM Portal uses RACI for various purposes. Its main use is for the purpose of identifying entity managers (Approvers). It is important that every model-configuration that you wish to audit be run through the RACI generator so that the Approvers will be listed correctly.

The RACI utility takes the data in the fields you identified when you defined the Universe as manager fields and tags them as the system's Accountables. The user manager data is taken from the configuration file's user database (*.udb). While any user can be accountable for multiple entities, each entity has only a single person accountable for it.

Note: Run the RACI utility before running a campaign, otherwise the system won't have users identified as entity Accountables, and won't be able to send the Approver tickets to the correct entity managers. If you didn't run RACI, you will either receive an error message, or all the entities will be listed with the campaign-owner for approval.

Create RACI

Note: Update the CA RCM user database before generating RACI for the universe.

Once a Universe is created, it is necessary to create its RACI configurations. The RACI configurations control the assignments of certification/attestation or approval tasks to their respective Accountable person. There are four RACI configurations, one for each of R,A,C,I. CA RCM automatically creates the A configuration, based on the Owner or Manager fields of the Universe.

To create the RACI configurations

1. On the Administration menu click Create RACI.
The Create RACI configurations screen opens.
2. Select a Universe from the drop-down.
3. Click Create RACI.

An appropriate notice appears when the process is completed.

Note: If the RACI configuration files become corrupted, you can access them through the CA RCM DNA module. On the File menu click Review Database. This allows you to view/delete the files.

More information:

[CA RCM Configuration Settings](#) (see page 228)

Synchronize RACI

Once the Universe's RACI configuration is created, it needs to be maintained in order to account for additional entities which are added to the universe, and therefore should also be reflected in the Universes' RACI.

When you import new users records into the Universe's configuration files, you can [automatically map them](#) (see page 200) to the Universe's RACI configuration files.

Note: RACI synchronization does not affect the links already present in the RACI configurations. It just adds new entity data or deletes entities that no longer exist. This means that if an existing entity's manager was changed, the Synchronize RACI utility will not update this information.

To synchronize the RACI configurations

1. On the Administration menu click Sync RACI.
The Sync RACI Configurations screen opens.
2. Select a Universe from the drop-down.
3. Click Sync RACI.

An appropriate notice appears when the process is completed.

TMS Administration

TMS stands for Ticket Management System. Tickets are work items used to track information, run jobs or notify users of events.

Tickets are generally not removed from the system (except when you click Cancel Process). They are archived. Tickets should be considered undeletable. But, nevertheless, in extreme circumstances, it is possible to delete all the system tickets.

Important! We highly recommend that you back up your system before deleting the system ticket and ticket types.

The TMS Administration utility provides you with two options:

- Delete All Tickets
- Delete All Tickets and Ticket Types

Click Delete next to the option that you want to execute. After deletion, a confirmation message appears.

More information:

[Using Tickets and the Inbox](#) (see page 23)

System Checkup

System checkup is an administrative tool that allows you to examine whether certain processes are working correctly. At this time, you can only check whether the CA RCM Portal's SMTP process is working correctly.

SMTP Checkup allows you to check two email systems:

TMS

The Ticket Management System's email connections

APP

General CA RCM Portal email connections.

To perform an SMTP checkup

1. On the Administration menu click System Checkup.
A list of System Checkup options appears.
2. Click SMTP Checkup.
3. The Checkup Options screen opens.
4. To check the TMS email system: Enter an email address in the Send Mail TMS box.
5. To check the App email system: Enter an email address in the Send Mail App.
6. Click Send.
The Executing bar appears.
7. Check the email box to see if the email arrived. If an email does not arrive, this indicates a problem that needs to be corrected.

How to Extract CA RCM Data

You can extract CA RCM data to the CA RCM External Report Database. Third-party reporting and data-mining applications can draw on this database to generate reports or perform analysis. Each extracted data snapshot is a static copy of CA RCM objects. CA RCM does not update the data snapshots after they are created.

You perform these procedures when you work with data extraction:

- [Enable the External Report Database](#) (see page 233)–Create the database and enable the feature on the CA RCM server.
- [Create an extraction profile](#) (see page 234) that defines the types of data files that are copied to the external report database.
- [Generate a data set, or snapshot](#) (see page 234), based on an extraction profile. You can schedule automatic generation of a data set at a fixed time or at recurrent intervals. Each data set is labeled with the name of the profile used to generate it and a timestamp.
- [Track data extraction jobs](#) (see page 235)–Data extraction jobs appear in the inbox of the administrator who runs/schedules them.
- [Delete profiles and data snapshots](#) (see page 237) when they are no longer needed. You can delete individual data sets, or schedule deletion at a future date.

Extraction profiles are similar to data connectors, and you use the job scheduling tools of the portal to initiate data snapshots like data connector jobs.

The data schema of the External Reporting Database is located in the **CA-RCM-rel#-Language-Files.zip** file of the CA RCM installation package.

How to Enable the External Report Database

Extracted data is stored in a dedicated SQL database on a Microsoft SQL Server database server. Follow these steps to enable the external report database:

1. Create the database on a Microsoft SQL Server.
 - When a Microsoft SQL Server hosts CA RCM databases, select the External Report Database option of the CA RCM installer to automatically create this database.
 - When an Oracle database server hosts CA RCM databases, create the External Report Database on a Microsoft SQL Server instance after you install CA RCM.

Note: For more information about creating the External report database, see the *Installation Guide*.

2. To enable data extraction, set the following CA RCM system parameter to True.

reportdb.enabled

Specifies whether CA RCM saves data snapshots to the external report database.

Valid values: True, False

Note: CA RCM resets this property to False when it cannot export a scheduled data snapshot to the database. If the connection to the database server is interrupted, reset the property to True when the connection is restored.

Create a Data Extraction Profile

Create a profile that specifies which data CA RCM copies to the external reporting database.

Note: You must have administrator-level rights in the CA RCM portal to perform this procedure.

To create a data extraction profile

1. Click Administration, External Report DB in the main menu of the portal.
The External Report Database main screen appears.
2. Click New Profile.
Note: To edit an existing export profile, click its name in the Profiles list.
The Basic Information screen appears.
3. Enter a name and brief description for the profile, and click Next.
The Parameters screen appears. All the files and data objects in the CA RCM databases are listed by type.
4. Click each tab and select the data files which you want to include in the extracted data.
5. (Optional) Click the Tickets tab and select the All Tickets option to include the entire ticket database.
Note: When you select a campaign, all its related tickets are included in the data snapshot, even if you do not select the All Tickets option.
6. Click Next.
The Overview screen appears.
7. Review the profile definition. If necessary, click Back to change settings.
8. Click Finish.
The profile is created. The External Report Database main screen appears. The new profile appears in the Profiles list.

Run or Schedule a Data Extraction Job

The data extraction job saves files to the External Report Database based on an extraction profile. Define at least one extraction profile before you run a data extraction job.

You can generate a single data snapshot, or schedule generation of data snapshots at regular intervals.

When you run a data extraction job, a tracking ticket appears in your inbox.

Note: You must have administrator-level rights in the CA RCM portal to perform this procedure.

To run or schedule a data extraction job

1. Click Administration, External Report DB from the main menu of the portal.

The External Report Database main screen appears.

2. Select *one* of the following options:

- Click Run Now in the Profiles list row of the the extraction profile you want the job to use.

The job begins immediately.

- To schedule future execution of a job, click Schedule in the Profiles list row of the the extraction profile you want the job to use.

The Schedule Extraction Task dialog appears.

Complete the following fields:

- **First execution**—Specifies the date and time at which the job is first run.
- **Number of additional repeats**—The number of times you want to run the job. Enter the value -1 to define an unending series.
- **Repeat interval**—The time period between executions in the series.

Click OK

The schedule is saved. CA RCM automatically initiates data snapshots according to the schedule.

Track Data Extraction Jobs

When you initiate data extraction to the CA RCM external reporting database, a Report DB Snapshot Extraction job ticket appears in your inbox. You can use this ticket to track generation of a data snapshot.

If you initiate immediate data extraction, the ticket appears immediately in the queue.

If you schedule a series of data snapshots, a new ticket appears for each snapshot when its data extraction begins.

You can also review and delete scheduled data extraction jobs in the Job Scheduling screen. Data extraction jobs are listed in the Job Scheduling screen with a Job Name as follows:

EXTRACTION.*extractionJobDetail*

The Job Class label has the value **ExtractionJob**.

Note: You must have administrator-level rights in the CA RCM portal to perform this procedure.

To track data extraction jobs

1. Run or schedule a data extraction job in the CA RCM portal.
2. Click Inbox on the main toolbar.

The Inbox screen appears. When a data extraction job is active, a Report DB Snapshot Extraction Ticket appears in the queue. The ticket title is the name of the data export profile on which the job is based.

3. Click the ticket title

The ticket opens.

The Ticket contains the following standard sections:

- The standard ticket header, which shows identification and status information
- The More section, which contains priority, severity, and ticket history information.
- The Advanced section, which lets you add attachments and notes.

4. Review the table in the Extraction Components section to track job progress.

Each row of the table lists a CA RCM data type, and the elapsed time taken to export all the files of this type that you selected. When extraction is complete, the Extraction State field has the value ENDED for all data types.

5. Open the Extraction Parameters for Profile section to review the scope of the extraction job.

The table lists the data types included in the data export profile that is used for this job, and the number of data files of each type that were selected for export.

6. Click Acknowledge when extraction of all data types is complete.

The ticket status changes to Completed and the ticket is removed from the active tickets queue.

Delete Data Extraction Profiles or Data Snapshots

Regularly scheduled data extractions can generate a large volume of data. Purge older data sets to reduce the size of the CA RCM external reporting database. You can also schedule automatic deletion at a future date and time.

Similarly, you may delete a data export profile if the data set it defines is no longer useful.

Note: You must have administrator-level rights in the CA RCM portal to perform this procedure.

To delete data extraction profiles or data snapshots

1. Click Administration, External Report DB from the portal main menu.
The External Report Database main screen appears.
2. (Optional) Delete an extraction profile:
 - a. Locate an export profile you want to delete in the Profiles list.
 - b. Click Delete in the row of that export profile.
The extraction profile is deleted.
3. (Optional) Delete a data snapshot:
 - a. Locate a data set you want to delete in the Snapshots list.
 - b. Click Delete in the row of that data set.
The data set is deleted.
4. (Optional) Schedule future deletion of a data snapshot:
 - a. Locate a data set you want to delete in the Snapshots list.
 - b. Click Schedule Delete in the row of that data set.
The Schedule Delete Snapshot dialog appears.
 - c. Specify the date and time at which to delete the snapshot, and click OK.
The snapshot is deleted at the scheduled date and time.

Chapter 13: About Security & Permissions

Corporate security has immense ramifications, especially when you consider the potential harm that could result from loss, alteration by unauthorized users, or misuse of data and resources. It is important that the software operates at a level of security that is consistent with the prevention of such potential harm.

The CA RCM Portal is accessible to both senior administrators and regular users. The different types of users have different needs and system usage. The CA RCM Portal has a comprehensive, Role-based, security and permissions structure aimed at ease-of-use on one hand, and maintaining appropriate security on the other hand.

This chapter discusses security issues and solutions of the CA RCM portal, both on the general level and on the user level.

This section contains the following topics:

[Security](#) (see page 239)

[Permissions](#) (see page 242)

Security

Software security is intended to prevent both unintentional and malicious harm. There are various ways of achieving this goal. This section presents the CA RCM Portal's solutions for specific security issues.

This section covers the following topics:

- Turning security on or off
- Authentication settings
- Encryption

More information:

[Turning Security On/Off](#) (see page 240)

[Authentication Settings](#) (see page 241)

[Encryption](#) (see page 241)

Turning Security On/Off

Software security can have one of two default positions:

Default Deny

Under these conditions, everything not explicitly permitted, is forbidden. While it may improve security, it does so at a cost in functionality.

Default Permit

Everything is permitted. The advantage of this kind of security operation is that it allows greater functionality, and it may be adequate for the initial phases of setting up and testing the system.

By default the CA RCM Portal's security parameter is set as disabled. This means that when a user logs in, using a recognized user name, the CA RCM Portal will not check the user's permissions: no limits will be placed on what is visible to the user. The user can see all the menus and menu options and the user can activate and use them all.

The security parameter located in the `eurekify.properties` file is:

```
sage.security.disable=true
```

When this property is set to `=False`, the system shifts to the Default Deny position and only what is explicitly permitted will be visible and enabled for the user.

More information:

[Permissions](#) (see page 242)

Authentication Settings

Authentication is the act of establishing that a user does indeed have security permission to gain access to the CA RCM Portal. The security parameters located in the `eurekify.properties` file governs the necessity of using a password to obtain access to the CA RCM Portal:

```
sage.security.disable.ADAuthentication=true
```

When this property is set to `=True`, the user does not have to use his/her established password in order to log in to the CA RCM Portal and any alphanumeric combination will allow them to gain entry.

When the property is set to `False`, only registered passwords will provide access to the CA RCM Portal. This means that there has to be a corporate Active Directory server that has a list of all the users and their passwords. When a user attempts to log in, the user and password are sent to the Active Directory server for authentication.

Encryption

When sending the user login and password data, it is recommended that this data be encrypted. The security parameter located in the `eurekify.properties` file is:

```
sage.security.disable.ssl.ADAuthentication=true
```

When this is set to `=True`, SSL authentication is disabled.

SSL, or Secure Sockets Layer technology enables encryption of sensitive information during transactions.

When the parameter is set to `=False`, that is SSL encryption is enabled, you have to also supply the keystore file:

```
sage.security.eurekify.keyStore.file=
```

The keystore file is a database that stores the private and public keys necessary for SSL encryption and decoding.

Permissions

When security is enabled, every action a user attempts is checked against the users' permissions. For this purpose, CA RCM.cfg provides a set of resources that govern the various permissions.

It should be noted, that the option that allows an Approver to view the contents of an Approver ticket, even if the Administrator did not give the Approver the appropriate permissions, sets up resources to handle this issue in the background. These permissions are limited to the specific campaign's requirements.

There are no permission filters for Delegate/Escalate.

More information:

[CA RCM Configuration Structure](#) (see page 242)

CA RCM Configuration Structure

This section discusses how the eurekify.cfg file's resource definitions impact a user's permissions. In general, various types of resources are pre-defined as permission related resources. The system recognizes three families of such resources:

- Link
- Doc_Access
- Filter

The easiest way to view and edit these resources is within the CA RCM DNA module.

Link Type Resources

Resources whose type is Link determine which menu options will be visible to each user.

The general syntax is:

[<Menu-Name>.<sub-menu>]

For example: [Self-Service.*] allows users linked to this resource permission to see and use all the available Self-Service menu items.

Adding [Exclude], after the square brackets, excludes a specific menu or menu item from the user's menu options.

Doc_Access Type Resources

DocAccess deals with permission to access documents: configuration, audit card, universe, and so on.

The general syntax is:

[<Document type>]

For example, [AUDITCARD] allows users linked to this resource permission to access this type of file.

Adding the modifier Read ([R]) or Read/Write ([RW]) sets the level of access to the files that the user is permitted to access. The value entered in the column Res Name 2 influences the level of permissions. * (asterisk) indicates – full permission for all such files, or a specific entity can be listed here, for example, a configuration name, a universe name.

Filter Type Resources

There are 3 types of filter resources:

- [Filter_User]
- [Filter_Role]
- [Filter_Resource]

The following columns provide important information when the resource's type is Filter:

Res Name 1

The resource name.

Res Name 2

The Universe name.

Res Name 3

Filter number.

Description

A description of the filter.

Type

The resource's type.

Filter1

A filter. For example:

```
(>(type=role)(A(type=user)(sageUser=$$PersonID$$$)))
```

More information:

[Filters](#) (see page 244)

Filters

This section explains the syntax of the filter used in the Filter type resources. The filtering is based on LDAP filtering of CA RCM entities.

The LDAP filter is designed implicitly define a set of CA RCM entities (users, roles or resources). The filter is based on the standard LDAP filter format with some minor adjustments.

Filter Format

The filter format relies on the LDAP pre-fix filter. The filter is constructed from an expression which, in turn, may be constructed from sub expressions.

Each expression should be surrounded by round brackets ("(",)") and should represent a set of Sage entities.

The simplest form of expression is a pair of a Sage entity field name and a regular expression representing desired values with an equality sign between them. For example: "(Location=Cayman)" or "(PersonID=86.*)".

Another simple form of expression is (Location>Cayman) which will bring users whose Location field lexicographically follows Cayman. Thus, an expressions such as:

```
(&(UserName>A)(UserName<B))
```

brings users whose Organization field is IN THE RANGE of A-B (inclusive).

Another type of simple expression is available for retrieval of relations. It starts with the ~ sign followed by brackets with a pair of relation type (user/role/resource) and the related entity name separated by an equals sign. For resources, three sets of brackets with the three names appear after the ~. For example:

```
(~(role=Cayman)) or ~(resname1=email)(resname2=outlook)(resname3=WinNT))
```

Expression may also have logical operations applied to them. The available operations are AND, OR and NOT. AND and OR are binary operations and should be applied to pairs of expressions while NOT is a unary operation. Operation symbols are:

& - AND

| - OR

! - NOT

Operator symbols are prefixes and should be placed before the expression/s

Usage examples:

"(&(Location=Cayman)(Organization=Finance))" - users in the Cayman finance office.

"(|(Country=US)(Country=UK))" – people in the US or the UK.

"(!(Active=false))" – Active users.

Filters may be as compound as necessary as long as they adhere to the above rules. For example:

"(&(|(Country=US)(Country=UK)) (&(!(Active=false))(Organization=Finance)))"

Are all the users which are from the US or the UK and are active users from the finance department.

Filter Extensions

These filter extensions are for internal use only (campaigns). Additional operators which involve the RACI model:

A – approved entities

> – links to approved entities

Usage examples:

- All roles whose approver is "AD1\Admin"
 - (A(type=role)(sageUser=AD1\Admin))
- All roles linked to users whose manager is "AD1\Admin"
 - (>(type=role)(A(type=user)(sageUser=AD1\Admin)))

Portal Structure (XML)

The Portal structure (the menus and sub-menus) is governed by an XML file: portal-structure.xml. A copy of the full xml document can be seen in Appendix C: Portal Structure (XML). These instructions determine the CA RCM Portal's menu structure

More information:

[Portal Structure \(XML\)](#) (see page 261)

Chapter 14: Troubleshooting

This chapter provides a list of the CA RCM Portal Error Messages

This section contains the following topics:

[Error Messages](#) (see page 247)

[Duplicating a Configuration](#) (see page 257)

Error Messages

CA RCM contains a system of messages that is intended to provide an alert when an activity cannot be completed as defined or if further information is needed to complete the activity: The following table displays typical messages and the type of action to perform:

Field	Code	Description
settings.raci.create.missingmanagers.errcode	adm001	It is recommended that all universe manager fields be filled before creating RACI, so that Accountable links can be automatically added.
settings.raci.create.alreadyexist.errcode	adm002	RACI configurations already exist for {0}
settings.raci.create.fail.errcode	adm003	failed to create RACI configurations for {0}
required.errcode	app001	field '{label}' is required.
iconverter.errcode	app002	'{input}' is not a valid {type}.
numbervalidator.range.errcode	app003	{input} is not between {minimum} and {maximum}.
numbervalidator.minimum.errcode	app004	'{input}' is smaller than the minimum of {minimum}.
numbervalidator.maximum.errcode	app005	'{input}' is larger than the maximum of {maximum}.
numbervalidator.positive.errcode	app006	'{input}' must be positive.
numbervalidator.negative.errcode	app007	'{input}' must be negative.
stringvalidator.range.errcode	app008	'{input}' is not between {minimum} and {maximum} characters long.

Field	Code	Description
stringvalidator.minimum.errcode	app009	'\${input}' is shorter than the minimum of \${minimum} characters.
stringvalidator.maximum.errcode	app010	'\${input}' is longer than the maximum of \${maximum} characters.
stringvalidator.exact.errcode	app011	'\${input}' is not exactly \${exact} characters long.
datevalidator.range.errcode	app012	'\${input}' is not between \${minimum} and \${maximum}.
datevalidator.minimum.errcode	app013	'\${input}' is less than the minimum of \${minimum}.
datevalidator.maximum.errcode	app014	'\${input}' is larger than the maximum of \${maximum}.
patternvalidator.errcode	app015	'\${input}' does not match pattern '\${pattern}'.
emailaddressvalidator.errcode	app016	'\${input}' is not a valid email address.
creditcardvalidator.errcode	app017	the credit card number is invalid.
urlvalidator.errcode	app018	'\${input}' is not a valid url.
equalinputvalidator.errcode	app019	'\${input0}' from \${label0} and '\${input1}' from \${label1} must be equal.
equalpasswordinputvalidator.errcode	app020	\${label0} and \${label1} must be equal.
user.count.roles.alert.description.errcode	apr001	user has {0} roles
user.count.resources.alert.description.errcode	apr002	user has {0} resources
role.count.users.alert.description.errcode	apr003	role has {0} users
role.count.children.alert.description.errcode	apr004	role has {0} children
role.count.resources.alert.description.errcode	apr005	role has {0} resources
resource.count.users.alert.description.errcode	apr006	resource has {0} users
resource.count.roles.alert.description.errcode	apr007	resource has {0} roles
campaignchoicesvalidator.errcode	arp001	please select at least one option for \${byfield} field.
configurationname.required.errcode	arp002	please select a configuration.
campaignname.required.errcode	arp003	please select a campaign.
byfield.required.errcode	arp004	please select the 'by field' parameter.

Field	Code	Description
auditcard.required.errcode	arp005	please select audit card.
sort.required.errcode	arp006	please select sorting method.
campaignfilteroption.required.errcode	arp007	please choose filtering type.
campaign.sendreminder.error.errcode	cmp001	send reminders was aborted, mail event is not active. update mailing parameter [tms.configuration.mail.events] in eurekaify.properties
campaign.text.campagin.errors.found.errcode	cmp002	errors found
campaign.error.nouniversesavailable.errcode	cmp003	no universes available
campaign.error.missingcampaigndescription.errcode	cmp004	missing campaign description
campaign.error.missingenddate.errcode	cmp005	missing end date
campaign.error.duedatemustbeinthefuture.errcode	cmp006	due date must be in the future
campaign.error.configurationmustbeselected.errcode	cmp007	configuration must be selected
campaign.error.racinotavailablefor.errcode	cmp008	raci not available for ({0})
campaign.error.campaignalreadyexists.errcode	cmp009	campaign [{0}] already exists
campaign.error.noaccess.errcode	cmp010	user {0} has no access to campaign {1}
settings.strings.ie.errors.missingname.errcode	cst001	missing name field.
settings.strings.ie.errors.missingdescription.errcode	cst002	missing description field.
settings.strings.ie.errors.namealreadyexist.errcode	cst003	duplicate name, name already in use.
settings.strings.ie.errors.missinguniverse.errcode	cst004	missing universe field.
settings.strings.ie.errors.missingsettings.errcode	cst005	was unable to find the settings xml file {0}.
settings.strings.ie.errors.missingmapping.errcode	cst006	was unable to find the mappings xml file {0}.
settings.strings.ie.errors.missingenrichment.errcode	cst007	was unable to find the enrichment file {0}.
settings.strings.ie.errors.missingpassword.errcode	cst008	missing password field.

Field	Code	Description
settings.strings.ie.errors.missingmaxduration.errcode	cst009	missing maxduration field.
settings.strings.ie.errors.errorparsingmaxduration.errcode	cst010	error parsing maxduration field, please use integer values.
settings.strings.ie.errors.missingconnectorclientclass.errcode	cst011	missing connector client class to use.
settings.strings.ie.errors.missingworkflowprocess.errcode	cst012	missing work flow process.
settings.strings.ie.errors.missingtickettype.errcode	cst013	missing ticket type.
dashboard.compliance.error.noname.errcode	dbc001	please enter all auditcard names
dashboard.compliance.error.multiname.errcode	dbc002	name {0} appears more than once
dashboard.compliance.error.nocard.errcode	dbc003	please enter all audit cards
dashboard.compliance.error.multicard.errcode	dbc004	auditcard {0} appears more than once
dashboard.compliance.error.nobpralerts.errcode	dbc005	auditcard {0} has no bpr alerts
entity.emptylist.errcode	eml001	no match was found
mail.builder.createticket.sage.errticket.subject.errcode	mal001	new error ticket, title:{3}
mail.builder.createticket.sage.errticket.body.errcode	mal002	a error ticket (id
properties.errormsg.propertyalreadyexists.errcode	prp001	the property {0}" already exists
properties.errormsg.unencryptedpropertyalreadyexists.errcode	prp002	an un-encrypted property [{0}] is already exists, please remove it first.
properties.errormsg.contcreateemptyproperty.errcode	prp003	can not create a property with a null/empty key.
loginpage.userauthentication.failed.errcode	prt006	failed to authenticate user, invalid user name/password
loginpage.connecttoauthenticationservice.failed.errcode	prt007	failed to connect to authentication service, please contact system administrator.
loginpage.userauthentication.failed.sageadmin.errcode	prt008	incorrect password for admin user.
loginpage.userauthentication.failed.sagebatch.errcode	prt009	incorrect password for batch user.
loginpage.userauthorization.failed.errcode	prt010	failed to authorize user: {0}, the user

Field	Code	Description
		does not exist in {1} configuration.
internalerrorpage.label.info1.errcode	prt011	an error has occurred. for more information please view the log file.
internalerrorpage.label.info2.errcode	prt012	to relogin please click here
sagemaster.headers.foundconflicts.errcode	sgm001	error! conflicts in the master configuration login field.
sagemaster.headers.countduplicates.errcode	sgm002	found {0} duplicate logins. please review:
selfservice.error.loading.bpr.errcode	sls001	could not load bpr file [{0}], proceeding without
selfservice.error.finding.bpr.errcode	sls002	no bpr file defined, proceeding without
selfservice.error.finding.universe.errcode	sls003	no universes available
selfservice.error.starting.approval.errcode	sls004	error starting approval process
selfservice.validate.descriptionrequired.errcode	sls005	description field is required
selfservice.validate.nouserisselected.errcode	sls006	no user is selected
selfservice.validate.norequestsmade.errcode	sls007	no requests made
selfservice.validate.missingraciconfigurations.errcode	sls008	missing raci configurations
selfservice.validate.errorgettingraciconfiguration.s.errcode	sls009	error getting raci configurations
selfservice.validate.missingaccountablefor.errcode	sls010	missing accountable for: {0}
selfservice.validate.racierrorfor.errcode	sls011	raci error for: {0}
settings.headers.editimportexportpage.error.errcode	ste001	error fetching connector object: {0}
settings.headers.edituniversepage.error.errcode	ste002	error fetching connector object
changeapproval.child.remove.user.role.info.title.rejected.errcode	tkt001	request to delete role {1} from user {1} - rejected.
changeapproval.child.remove.user.role.info.title.failed.errcode	tkt002	request to delete role {0} from user {1} - failed.
changeapproval.child.remove.user.role.notification.title.errcode	tkt003	request to delete role {1} from user {0} is already in process.
changeapproval.child.add.user.resource.info.title.rejected.errcode	tkt005	request to add resource {1} to user {1} - rejected.
changeapproval.child.add.user.resource.info.title	tkt006	request to add resource {0} to user

Field	Code	Description
.failed.errcode		{1} - failed.
changeapproval.child.add.user.resource.info.description.rejected.errcode	tk007	the request to add resource {1} to user {0} was rejected - request was submitted on universe {2} from {3}
changeapproval.child.add.user.resource.info.description.failed.errcode	tk008	the request to add resource {1} to user {0} failed - request was submitted on universe {2} from {3}
changeapproval.child.remove.user.resource.info.title.rejected.errcode	tk009	request to delete resource {1} from user {0} - rejected.
changeapproval.child.remove.user.resource.info.title.failed.errcode	tk010	request to delete resource {1} from user {0} - failed.
changeapproval.child.remove.user.resource.info.description.rejected.errcode	tk011	the request to delete resource {1} from user {0} was rejected - request was submitted on universe {2} from {3}
changeapproval.child.remove.user.resource.info.description.failed.errcode	tk012	the request to delete resource {1} from user {0} failed - request was submitted on universe {2} from {3}
changeapproval.child.remove.user.resource.notification.title.errcode	tk013	request to delete resource {1} from user {0} is already in process.
changeapproval.child.remove.user.resource.notification.description.errcode	tk014	the request to delete resource {1} from user {0} is already in process - request was submitted on universe {2} from {3}
changeapproval.child.add.role.role.info.title.rejected.errcode	tk015	request to add role {0} to role {1} - rejected.
changeapproval.child.add.role.role.info.title.failed.errcode	tk016	request to add role {0} to role {1} - failed.
changeapproval.child.add.role.role.info.description.rejected.errcode	tk017	the request to add role {0} to role {1} was rejected - request was submitted on universe {2} from {3}
changeapproval.child.add.role.role.info.description.failed.errcode	tk018	the request to add role {0} to role {1} failed - request was submitted on universe {2} from {3}
changeapproval.child.add.role.role.notification.title.errcode	tk019	request to add role {0} to role {1} is already in process.
changeapproval.child.add.role.role.notification.description.errcode	tk020	the request to add role {0} to role {1} is already in process - request was submitted on universe {2} from {3}

Field	Code	Description
changeapproval.child.remove.role.role.info.title.rejected.errcode	tk021	request to delete role {0} from role {1} - rejected.
changeapproval.child.remove.role.role.info.title.failed.errcode	tk022	request to delete role {0} from role {1} - failed.
changeapproval.child.remove.role.role.info.description.rejected.errcode	tk023	the request to delete role {0} from role {1} was rejected - request was submitted on universe {2} from {3}
changeapproval.child.remove.role.role.info.description.failed.errcode	tk024	the request to delete role {0} from role {1} failed - request was submitted on universe {2} from {3}
changeapproval.child.remove.role.role.notification.title.errcode	tk025	request to delete role {0} from role {1} is already in process.
changeapproval.child.remove.role.role.notification.description.errcode	tk026	the request to delete role {0} from role {1} is already in process - request was submitted on universe {2} from {3}
changeapproval.child.add.role.resource.info.title.rejected.errcode	tk027	request to add resource {1} to role {1} - rejected.
changeapproval.child.add.role.resource.info.title.failed.errcode	tk028	request to add resource {0} to role {1} - failed.
changeapproval.child.add.role.resource.info.description.rejected.errcode	tk029	the request to add resource {1} to role {0} was rejected - request was submitted on universe {2} from {3}
changeapproval.child.add.role.resource.info.description.failed.errcode	tk030	the request to add resource {1} to role {0} failed - request was submitted on universe {2} from {3}
changeapproval.child.add.role.resource.notification.title.errcode	tk031	request to add resource {1} to role {0} is already in process.
changeapproval.child.add.role.resource.notification.description.errcode	tk032	the request to add resource {1} to role {0} is already in process - request was submitted on universe {2} from {3}
changeapproval.child.remove.role.resource.info.title.rejected.errcode	tk033	request to delete resource {1} from role {1} - rejected.
changeapproval.child.remove.role.resource.info.title.failed.errcode	tk034	request to delete resource {0} from role {1} - failed.
changeapproval.child.remove.role.resource.info.description.rejected.errcode	tk035	the request to delete resource {1} from role {0} was rejected - request was submitted on universe {2} from {3}

Field	Code	Description
changeapproval.child.remove.role.resource.info.description.failed.errcode	tkk036	the request to delete resource {1} from role {0} failed - request was submitted on universe {2} from {3}
changeapproval.child.remove.role.resource.notification.title.errcode	tkk037	request to delete resource {1} from role {0} is already in process.
changeapproval.child.remove.role.resource.notification.description.errcode	tkk038	the request to delete resource {1} from role {0} is already in process - request was submitted on universe {2} from {3}
changeapproval.child.role.task.addroletoraci.description.errcode	tkk039	to continue please choose an accountable user to {0} role
changeapproval.child.remove.user.role.notification.description.errcode	tkk094	the request to delete role {1} from user {0} is already in process - request was submitted on universe {2} from {3}
login.errors.invalidcredentials.errcode	tms001	user/password not found.
login.errors.invalidcredentials.errcode	tms001	try wicket/wicket as the user name/password combination
page.admin.failuremessage.errcode	tms002	{0} failed.
error.validate.optionvalue.errcode	tms003	the value {0} is not allowed in {1}.
error.validate.command.notfound.errcode	tms004	the command id {0} was not found.
error.validate.command.disabled.errcode	tms005	the command id {0} is not enabled.
error.addattachment.noname.errcode	tms006	fail to save attachment, please fill the field name.
error.filter.errcode	tms007	the filter '{0}' has a syntax error. {1}
error.filter.resultempty.errcode	tms008	the user does not exist.
error.command.revokecmd.errcode	tms009	fail to revoke ticket {0}, missing job tickets {1}.
error.command.revokecmd.msg2.errcode	tms010	fail to revoke ticket {0} with job tickets {1}, there are {2} activity tickets outside the ticket tree.
error.command.linkcommands.errcode	tms011	fail to create commands:{0}, {1}
error.command.startjobcommand.errcode	tms012	fail to start job for ticket {0}, ticket has already reference for job {1}
error.command.startjobcommand.checkjobticketexists.errcode	tms013	fail to commit activity [checkjobticketexists] in job [{1}] of ticket {0}, check tms port in workpoint

Field	Code	Description
		wftms web service.
error.workflow.connection.errcode	tms014	fail to connect to workpoint url:{0}, info:{1}
error.service.createconsulttickets.errcode	tms015	no ticket parent!
error.service.createconsulttickets2.errcode	tms016	fail to find consulting users, {0}
error.service.createconsulttickets3.errcode	tms017	fail to create consulting tickets. {0}
error.service.validatevalue.errcode	tms018	fail to update field {0} with value {1} in ticket type {2}
error.command.saveticket.optimisticclockexception.errcode	tms019	the ticket was updated by another user, please reopen ticket.
error.validate.valuelength.errcode	tms020	validation fail for value:{0} cannot be longer then {1}
error.validate.date.errcode	tms021	fail to parse date: {0}"
error.batchtask.errcode	tms022	[{6}] fail to run batch actionname
error.batchtask.startjob.errcode	tms023	action {0} of job {2} failed. retry count:{1}
error.update.ticket.errcode	tms024	cannot update the ticket [id
error.campaignnamenotfound.errcode	tms025	campaign {0} not found.
page.recordnotfound.message.errcode	tms026	{0} was not found in {1}
page.internalerror.info1.errcode	tms027	an error has occurred. for more information please view the log file.
page.internalerror.info2.errcode	tms028	null
page.expirederror.info1.errcode	tms029	your session has expired, please login again.
page.expirederror.info2.errcode	tms030	null
error.workpoint.dbconnection.errcode	tms031	workpoint database connection is closed.
text.dialogs.runfailed.errcode	txd001	failed to run {0}, please watch log files.
text.dialogs.runfailed.errcode	txs002	failed to run {0}, please watch log files.
settings.strings.universe.masterequalmodel.errcode	ust001	warning!!! master and model configurations are the same.
settings.strings.universes.errors.missingname.errcode	ust002	missing name field.

Field	Code	Description
settings.strings.universes.errors.missingdescription .errcode	ust003	missing description field.
settings.strings.universes.errors.namealreadyexists .errcode	ust004	duplicate name, name already in use.
settings.strings.universes.errors.missingmaster .errcode	ust005	missing master configuration name field.
settings.strings.universes.errors.missingmodel .errcode	ust006	missing model configuration name field.
settings.strings.universes.errors.missingauditsettingsfile.errcode	ust007	was unable to find the audit settings file {0}.
settings.strings.universes.errors.masterisnotreadonly .errcode	ust008	the master configuration ({0}) is not read only.
settings.strings.universes.errors.masterhasparent .errcode	ust009	the master configuration ({0}) has a parent configuration.
settings.strings.universes.errors.masternotlogged .errcode	ust010	the model configuration ({0}) is not logged.
settings.strings.universes.errors.modelisnotreadonly .errcode	ust011	the model configuration ({0}) is not read only.
settings.strings.universes.errors.modelhasparent .errcode	ust012	the model configuration ({0}) has a parent configuration.
settings.strings.universes.errors.modelnotlogged .errcode	ust013	the model configuration ({0}) is not logged.
settings.strings.universes.errors.errorswasfound .errcode	ust014	the following issues were found:
settings.strings.universes.errors.wouldliketoauto fix .errcode	ust015	would you like to auto-fix them?
error.workpoint.dbconnection.errcode	wp001	workpoint database connection is closed.

Duplicating a Configuration

In the course of your work with the CA RCM Portal, you may need to duplicate a configuration, whether to use while learning the CA RCM Portal, or because you need to generate a master/model configuration set that can be used as the base line for a Universe you will create later in the CA RCM Portal. This set of configurations can be based on an existing configuration, which you would like to keep as-is. The new configuration pair can also be based on a partial configuration that you wish to investigate.

A CA RCM configuration consists of a configuration file (.cfg) a user database file (.udb) and a resource database file (.rdb). The configuration file contains references to the user and resource database files. Therefore, you cannot use the operating system's copy/paste/rename functions in order to duplicate a configuration. You need to actually change the content of the configuration file during the process.

You can use the Trim Configuration process provided by the CA RCM DNA module to duplicate a configuration. This allows you to generate a configuration in which the new (duplicate) users and resource database files are referenced from within the new configuration file.

Note: Refer to the *DNA User Guide* for details of the Trim Configuration function.

Important! We recommend that when generating duplicate files for use with a Universe that you use the terms Master/Model as part of the configuration file names.

Appendix A: CA RCM Properties

This section contains the following topics:

[tms.delegate.filter](#) (see page 259)

[tms.escalate.filter](#) (see page 260)

[tms.campaign.\[campaign-type\].reassign.filter](#) (see page 260)

tms.delegate.filter

Used for filtering the delegate option user list. Comprises three options:

Description	Default delegate filter
Property	tms.delegate.filter
Example	tms.delegate.filter=GFilter=(Organization=\$\$owner.Organization\$\$)
Description	Ticket type filter
Property	tms.delegate.filter.TicketType.SAGE.ChangeApprovalParentTicket
Example	tms.delegate.filter.TicketType.SAGE.ChangeApprovalParentTicket=GFilter=(Organization=cookingdept)
Description	Ticket name filter
Property	tms.delegate.filter.LinkUser-Role
Example	tms.delegate.filter.LinkUser-Role=GFilter=(Email=ssimhi@eurekify.com)

The "name" property (if defined) takes precedence over "type" which in turn takes precedence over the default delegate property.

tms.escalate.filter

Used for filtering the escalate option user list. Comprises three options:

Description	Default escalate filter
Property	tms.escalate.filter
Example	tms.escalate.filter=GFilter=(Organization=\$\$owner.Organization\$\$)
Description	Ticket type filter
Property	tms.escalate.filter.TicketType.SAGE.ChangeApprovalParentTicket
Example	tms.escalate.filter.TicketType.SAGE.ChangeApprovalParentTicket=GFilter=(Organization=cookingdept)
Description	Ticket name filter
Property	tms.escalate.filter.LinkUser-Role
Example	tms.escalate.filter.LinkUser-Role=GFilter=(Email=ssimhi@eurekify.com)

tms.campaign.[campaign-type].reassign.filter

Used for filtering the reassign option user list. Comprises three options:

Description	Reassign filter
Property	tms.campaign.[campaign-type].reassign.filter
Example	tms.campaign.userCertification.reassign.filter=GFilter=(Organization=\$\$owner.Organization\$\$) tms.campaign.roleCertification.reassign.filter=GFilter=(Organization=\$\$owner.Organization\$\$) tms.campaign.resourceCertification.reassign.filter=GFilter=(Organization=\$\$owner.Organization\$\$)

Appendix B: Portal Structure (XML)

This section contains the following topics:

[Sample Portal Structure XML](#) (see page 262)

Sample Portal Structure XML

```
<?xml version="1.0" standalone="yes" ?>
<!DOCTYPE portal (View Source for full doctype...) >
- <portal>
- <tag id="HomePage">
  <type>internal</type>
  <label>Home</label>
  <data>com.eurekify.web.portal.homepage.HomePage</data>
  <checkPermission>>false</checkPermission>
</tag>
- <tag id="TmsSystem">
  <type>external</type>
  <data>$$$SAGE_SERVICE_URL$$tms/ui/credential</data>
  <checkPermission>>true</checkPermission>
- <tag id="DefaultTickets">
  <type>external</type>
  <label>Open/New/Done Tickets</label>
  <data>$$$SAGE_SERVICE_URL$$tms/ui/credential?filter=DEFAULT </data>
  <checkPermission>>false</checkPermission>
</tag>
- <tag id="NewTickets">
  <type>external</type>
  <label>New Tickets</label>
  <data>$$$SAGE_SERVICE_URL$$tms/ui/credential?filter=STATE_NEW</data>
  <checkPermission>>false</checkPermission>
</tag>
- <tag id="overDue">
  <type>external</type>
  <label>Over Due</label>
  <data>$$$SAGE_SERVICE_URL$$tms/ui/credential?filter=OVER_DUE</data>
  <checkPermission>>false</checkPermission>
</tag>
- <tag id="approverTickets">
  <type>external</type>
  <label>Approver Tickets</label>
  <data>$$$SAGE_SERVICE_URL$$tms/ui/credential?filter=APPROVER_TICKET</data>
  <checkPermission>>false</checkPermission>
</tag>
- <tag id="campaignTickets">
  <type>external</type>
  <label>Campaign Tickets</label>
  <data>$$$SAGE_SERVICE_URL$$tms/ui/credential?filter=CAMPAIGN_TICKETS</data>
  <checkPermission>>false</checkPermission>
</tag>
- <tag id="archivedTickets">
  <type>external</type>
  <label>Archived Tickets</label>
  <data>$$$SAGE_SERVICE_URL$$tms/ui/credential?filter=STATE_ARCHIVED</data>
```

```

<checkPermission>false</checkPermission>
</tag>
</tag>
- <tag id="DashBoard">
<type>external</type>
<label>Dashboards</label>
- <data>
- <!-- http://localhost:8080/group/eurekify/configuration?usertoken=$$USER_TOKEN$$-->

/group/eurekify/configuration?usertoken=$$USER_TOKEN$$
</data>
<checkPermission>true</checkPermission>
</tag>
- <tag id="SelfService">
<type>mark</type>
<label>Self Service</label>
<checkPermission>true</checkPermission>
- <tag id="manageTeamRoles">
<type>internal</type>
<label>Manage My Team's Role Assignments</label>
<data>com.eurekify.web.selfservice.RolesTeamServicePage</data>
<checkPermission>true</checkPermission>
</tag>
- <tag id="manageSelfRoles">
<type>internal</type>
<label>Manage My Roles Assignments</label>
<data>com.eurekify.web.selfservice.RolesSelfServicePage</data>
<checkPermission>true</checkPermission>
</tag>
- <tag id="manageTeamResources">
<type>internal</type>
<label>Manage My Team's Resources Assignments</label>
<data>com.eurekify.web.selfservice.ResourcesTeamServicePage</data>
<checkPermission>true</checkPermission>
</tag>
- <tag id="manageSelfResources">
<type>internal</type>
<label>Manage My Resources Assignments</label>
<data>com.eurekify.web.selfservice.ResourcesSelfServicePage</data>
<checkPermission>true</checkPermission>
</tag>
- <tag id="requestNewRole">
<type>internal</type>
<label>Request a New Role Definition</label>
<data>com.eurekify.web.rolerequests.RoleDefinitionPage</data>
<checkPermission>true</checkPermission>
</tag>
- <tag id="requestUpdateRole">
<type>internal</type>

```

```
<label>Request Changes to a Role Definition</label>
<data>com.eurekify.web.rolerequests.UpdateRolePage</data>
<checkPermission>true</checkPermission>
</tag>
</tag>
- <tag id="EntityBrowser">
<type>internal</type>
<label>Entity Browser</label>
<data>com.eurekify.web.entitybrowser.EurekifyBrowserPage</data>
<checkPermission>true</checkPermission>
</tag>
- <tag id="Reports">
<type>mark</type>
<label>Reports</label>
<checkPermission>true</checkPermission>
- <tag id="ConfigReports">
<type>internal</type>
<label>Configuration Reports</label>
<checkPermission>true</checkPermission>
- <tag id="ConfigurationProperties">
<type>report</type>
<label>Configuration Properties</label>
<data>com.eurekify.web.reports.parameters.universeconfigurationreports.ConfigurationPropertiesParametersPage</data>
<checkPermission>true</checkPermission>
</tag>
- <tag id="ConfigurationUsersAttributes">
<type>report</type>
<label>Configuration Users Attributes</label>
<data>com.eurekify.web.reports.parameters.configurationattributes.users.ConfigurationUsersAttributesParametersPage</data>
<checkPermission>true</checkPermission>
</tag>
- <tag id="ConfigurationRolesAttributes">
<type>report</type>
<label>Configuration Roles Attributes</label>
<data>com.eurekify.web.reports.parameters.configurationattributes.roles.ConfigurationRolesAttributesParametersPage</data>
<checkPermission>true</checkPermission>
</tag>
- <tag id="ConfigurationResourcesAttributes">
<type>report</type>
<label>Configuration Resources Attributes</label>
<data>com.eurekify.web.reports.parameters.configurationattributes.resources.ConfigurationResourcesAttributesParametersPage</data>
<checkPermission>true</checkPermission>
</tag>
- <tag id="ConfigurationUsersFull">
<type>report</type>
<label>Configuration Users Full</label>
```



```

<data>com.eurekify.web.reports.parameters.configurationattributes.users.ConfigurationUsersFullParametersPage</data>
<checkPermission>true</checkPermission>
</tag>
- <tag id="ConfigurationRolesFull">
<type>report</type>
<label>Configuration Roles Full</label>
<data>com.eurekify.web.reports.parameters.configurationattributes.roles.ConfigurationRolesFullParametersPage</data>
<checkPermission>true</checkPermission>
</tag>
- <tag id="ConfigurationResourcesFull">
<type>report</type>
<label>Configuration Resources Full</label>
<data>com.eurekify.web.reports.parameters.configurationattributes.resources.ConfigurationResourcesFullParametersPage</data>
<checkPermission>true</checkPermission>
</tag>
</tag>
- <tag id="PrivilegesQualityManagement">
<type>internal</type>
<label>Privileges Quality Management</label>
<checkPermission>true</checkPermission>
- <tag id="OverlappingRolesByUsers">
<type>report</type>
<label>Overlapping Roles By Users</label>
<data>com.eurekify.web.reports.parameters.overlappingroles.OverlappingRolesByUsersParametersPage</data>
<checkPermission>true</checkPermission>
</tag>
- <tag id="OverlappingRolesByResources">
<type>report</type>
<label>Overlapping Roles By Resources</label>
<data>com.eurekify.web.reports.parameters.overlappingroles.OverlappingRolesByResourcesParametersPage</data>
<checkPermission>true</checkPermission>
</tag>
- <tag id="SuspectedConnectionsUserRes">
<type>report</type>
<label>Suspected Connections User Resource</label>
<data>com.eurekify.web.reports.parameters.suspectedconnections.SuspectedConnectionsUserResParametersPage</data>
<checkPermission>true</checkPermission>
</tag>
- <tag id="SuspectedConnectionsUserRole">
<type>report</type>
<label>Suspected Connections User Role</label>
<data>com.eurekify.web.reports.parameters.suspectedconnections.SuspectedConnectionsUserRoleParametersPage</data>
<checkPermission>true</checkPermission>
</tag>
- <tag id="PrivilegesStatisticsReportForUsers">
<type>report</type>

```

```
<label>Privileges Statistics For Users Report</label>
<data>com.eurekify.web.reports.parameters.universeconfigurationreports.PrivilegesStatisticsForUsersParametersPage</data>
<checkPermission>true</checkPermission>
</tag>
- <tag id="PrivilegesStatisticsReportForRoles">
  <type>report</type>
  <label>Privileges Statistics For Roles Report</label>
  <data>com.eurekify.web.reports.parameters.universeconfigurationreports.PrivilegesStatisticsForRolesParametersPage</data>
  <checkPermission>true</checkPermission>
  </tag>
- <tag id="PrivilegesStatisticsReportForResources">
  <type>report</type>
  <label>Privileges Statistics For Resources Report</label>
  <data>com.eurekify.web.reports.parameters.universeconfigurationreports.PrivilegesStatisticsForResourcesParametersPage</data>
  <checkPermission>true</checkPermission>
  </tag>
- <tag id="AuditBasicAlerts">
  <type>report</type>
  <label>Audit Basic Alerts</label>
  <data>com.eurekify.web.reports.parameters.auditalerts.AuditBasicAlertsParametersPage</data>
  <checkPermission>true</checkPermission>
  </tag>
- <tag id="RoleManagement">
  <type>internal</type>
  <label>Role Management</label>
  <checkPermission>true</checkPermission>
- <tag id="RolesAnalysisReport">
  <type>report</type>
  <label>Roles Analysis Report</label>
  <data>com.eurekify.web.reports.parameters.roleanalysis.RolesAnalysisParametersPage</data>
  <checkPermission>true</checkPermission>
  </tag>
- <tag id="RoleEngineeringMethodologies">
  <type>report</type>
  <label>Role Modeling Methodologies Comparison</label>
  <data>com.eurekify.web.reports.parameters.roleengineering.RoleEngineeringParametersPage</data>
  <checkPermission>true</checkPermission>
  </tag>
- <tag id="PolicyManagement">
  <type>internal</type>
  <label>Policy Management</label>
  <checkPermission>true</checkPermission>
- <tag id="PolicyVerificationReport">
  <type>report</type>
```

```
<label>Policy Verification Report</label>
<data>com.eurekify.web.reports.parameters.universeconfigurationreports.PolicyVerificationParametersPage</data>
<checkPermission>true</checkPermission>
</tag>
</tag>
- <tag id="Campaigns">
  <type>internal</type>
  <label>Campaigns</label>
  <checkPermission>true</checkPermission>
- <tag id="FullCertificationReport">
  <type>report</type>
  <label>Full Certification Report</label>
  <data>com.eurekify.web.reports.parameters.campaign.FullCertificationParametersPage</data>
  <checkPermission>true</checkPermission>
</tag>
- <tag id="CertificationProgressReport">
  <type>report</type>
  <label>Certification Progress Report</label>
  <data>com.eurekify.web.reports.parameters.campaign.CertificationProgressParametersPage</data>
  <checkPermission>true</checkPermission>
</tag>
</tag>
</tag>
- <tag id="Administration">
  <type>mark</type>
  <label>Administration</label>
  <data>com.eurekify.web.AdministrationPage</data>
  <checkPermission>true</checkPermission>
- <tag id="SetCampaign">
  <type>internal</type>
  <label>Add Campaign</label>
  <data>com.eurekify.web.campaign.SetCampaignPage</data>
  <checkPermission>false</checkPermission>
</tag>
- <tag id="ScheduledTasksPage">
  <type>internal</type>
  <label>Job Scheduler</label>
  <data>com.eurekify.web.ScheduledTasksPage</data>
  <checkPermission>true</checkPermission>
</tag>
- <tag id="TxLogPage">
  <type>internal</type>
  <label>TxLog Page</label>
  <data>com.eurekify.web.TxLogPage</data>
  <checkPermission>true</checkPermission>
</tag>
- <tag id="LoadCachePage">
  <type>internal</type>
  <label>Load Cache</label>
```

```
<data>com.eurekify.web.LoadCachePage</data>
</tag>
- <tag id="ClearCachesPage">
  <type>internal</type>
  <label>Clear Cache</label>
  <data>com.eurekify.web.ClearCachesPage</data>
  </tag>
- <tag id="CreateRaciPage">
  <type>internal</type>
  <label>Create RACI</label>
  <data>com.eurekify.web.CreateRaciPage</data>
  <checkPermission>true</checkPermission>
  </tag>
- <tag id="SyncRaciPage">
  <type>internal</type>
  <label>Sync RACI</label>
  <data>com.eurekify.web.SyncRaciPage</data>
  <checkPermission>true</checkPermission>
  </tag>
- <tag id="TmsAdmin">
  <type>external</type>
  <label>TMS Administration</label>
  <data>$$$SAGE_SERVICE_URL$$tms/ui/admin</data>
  <checkPermission>true</checkPermission>
  </tag>
- <tag id="Settings">
  <type>internal</type>
  <label>Settings</label>
  <checkPermission>true</checkPermission>
- <tag id="ConnectorSettings">
  <type>internal</type>
  <label>Connector Settings</label>
  <data>com.eurekify.web.settings.ConnectorsSettingsPage</data>
  <checkPermission>true</checkPermission>
  </tag>
- <tag id="UniversesSettings">
  <type>internal</type>
  <label>Universe Settings</label>
  <data>com.eurekify.web.settings.UniversesSettingsPage</data>
  <checkPermission>true</checkPermission>
  </tag>
- <tag id="PropertiesSettings">
  <type>internal</type>
  <label>Properties Settings</label>
  <data>com.eurekify.web.properties.PropertiesPage</data>
  <checkPermission>true</checkPermission>
  </tag>
- <tag id="CommonPropertiesSettings">
  <type>internal</type>
```

```
<label>Common Properties Settings</label>
<data>com.eurekify.web.properties.CommonPropertiesPage</data>
<checkPermission>true</checkPermission>
</tag>
- <tag id="AuditPropertiesSettings">
<type>internal</type>
<label>Audit Properties Settings</label>
<data>com.eurekify.web.properties.AuditPropertiesPage</data>
<checkPermission>true</checkPermission>
</tag>
</tag>
- <tag id="SageMaster">
<type>internal</type>
<label>Eurekify Configuration Settings</label>
<checkPermission>false</checkPermission>
- <tag id="UpdateSagemaster">
<type>internal</type>
<label>Update Eurekify configuration with universe users</label>
<data>com.eurekify.web.sageMaster.UpdateSageMasterPage</data>
<checkPermission>true</checkPermission>
</tag>
</tag>
- <tag id="Checkup">
<type>internal</type>
<label>System Checkup</label>
<checkPermission>false</checkPermission>
- <tag id="MailCheckup">
<type>internal</type>
<label>SMTP Checkup</label>
<data>com.eurekify.web.checkup.CheckupPage</data>
<checkPermission>true</checkPermission>
</tag>
</tag>
</tag>
</portal>
```


Appendix C: CA RCM Configuration Data Formats

CA RCM uses three separate but related files in text-based comma-separated format to represent a configuration. These files are:

- Users database file
- Resources database file
- Configuration file

The users and resources database files contain the basic features of users and resources. The configuration file contains the dynamic parts of a configuration; that is, the roles and relationships/connections.

This section contains the following topics:

[Users Database File](#) (see page 271)

[Resource Database File](#) (see page 272)

[Configuration File](#) (see page 273)

Users Database File

User database file names end with the .udb suffix. Each user is represented in this file by one line, which includes comma-separated values for the following fields (in this order):

- PersonID (the key)
- User name
- Organization name
- Organization type
- (Optional) an unlimited number of additional fields.

Although they are optional, CA RCM requires you to specify fields for the following types of user information when you define a universe. Define these fields in .udb files that form the basis for a configuration file in a universe.

- LoginID
- User email
- ManagerID

Example: User Database File

The following sample .udb file contains 3 user records.

```
PersonID,UserName,OrgName,OrgType,Country,Location,ManagerID,email,LoginID,  
"52656727","Rodman Adam","System  
Management","Corporate","US","Pennsylvania","54672910","52656727@company.com","IBMR50\\Rodman  
Adam",  
"54672910","Cooper Amos","IT  
Security","Corporate","US","Pennsylvania","64646410","54672910@company.com","IBMR50\\Cooper Amos",  
"64646410","Herman Barbara","Operations","Corporate","US","New  
Jersey","64646410","64646410@company.com","IBMR50\\Herman Barbara",
```

Resource Database File

Resource database file names end with the .rdb suffix. Each resource is represented in this file by one line, which includes comma-separated values for the following fields (in this order):

- Resource Name 1 (ResName1)
- Resource Name 2 (ResName1)
- Resource Name 3 (ResName1)
- (Optional) An unlimited number of additional fields

The ResName fields typically map to the endpoint or application group of the resource.

Although they are optional, CA RCM requires you to specify fields for the following types of resource information when you define a universe. Define these fields in .rdb files that form the basis for a configuration file in a universe.

- Application
- ManagerID

Example: Resource Database File

The following sample file contains 3 resource records.

```
ResName1,ResName2,ResName3,Description,ManagerID-Owner,Location,  
"SYS1","RACFPROD","RACF22","Production RACF","77292450","Irvine,CA",  
"Domain Users","NT5AVE","WinNT","Active Directory ","91236370","Houson,TX",  
"DEVELOP","RACFPROD","RACF22","Production RACF","77292450","Irvine,CA",
```


Configuration File

Configuration file names end with the .cfg suffix. The configuration file refers to a user database file and a resource database file. It contains role definitions and links between users, roles, and resources.

Note: Multiple configurations may share the same users and resource database files.

The configuration file has the following structure:

- A header section lists the owner and modification history of the file. The first two lines in the file specify the user and resource database files that the configuration references. These lines have the following format:

```
UsersDB,udb_pathname
ResDB,rdb_pathname
```

Note: *udb_pathname* is the pathname of the referenced user database file, and *rdb_pathname* is the pathname of the referenced resource database file.

- User entity declarations define a subset of users from the referenced user database file. Each line defines a single user, with the following format:

```
User, udb_record, PersonID
```

Note: *udb_record* is the index value of a record in the user database file. The first user record in the .udb file has an index value of zero. *PersonID* is the value of the PersonID field in the referenced user record.

- Resource entity declarations define a subset of resources from the referenced resource database file. Each line defines a single resource, with the following format:

```
Res, rdb_record, ResName1, ResName2, ResName3
```

Note: *rdb_record* is the index value of a record in the resource database file. The first user record in the .rdb file has an index value of zero. *ResName1*, *ResName2*, *ResName3* are the values of the corresponding mandatory fields in the referenced resource record.

- Role declarations define a role in terms of users, resources, or other roles in the configuration. Each declaration defines a single role in one line, with the following format:

```
Role,roleID,roleName,roleDescription,roleOrganization,roleOwner
```

Note: *roleID* is the numerical identifier CA RCM assigns to the role, *roleName* is the unique name of the role, *roleDescription* is a text description of the role, *roleOrganization* is the organization associated with the role, and *roleOwner* is the user that owns the role.

- Link declarations define role contents and user privileges as a set of links between the declared user, role and resource entities. Each line defines a single link, with the following format:

Link_type,Entity1,Entity2

Note: *Link_type* specifies the type of link. *Entity1* and *Entity2* specify the linked entities, using the record index of a user or resource entity, or the roleID of a role entity.

The *Link_type* string can have the following values:

- User-Res–user-resource link
- User-Role–user-role link
- Role-Res–role-resource link
- Role-Role–role-role link (parent-child link within the role hierarchy)

Entities must be listed in order. For example, in a User-Res declaration, the first entity is a user record, and the second entity is a resource record. In a Role-Role link, the first entity is the roleID of the parent role, and the second entity is the roleID of the child role.

Example: Configuration File

Configuration files are typically much larger than this sample. In this example, role 1001 has only one resource, role 1014 has two resources, and role 1015 includes both role 1001 and role 1014 as children.

```

UsersDB,.\UsersDB.udb
ResDB,.\ResDB.rdb
CreateDate,03/09/2007 12:27
ModifyDate,03/09/2007 12:27
StatusDate,17/04/2007 15:36
Owner1,Ilan Sharoni
Organization1,Company
Owner2,
Organization2,
Operation1,
Operation2,
Operation3,
Status,
ParentConfigName,SQL://(local).sdb/ConfigWithRoles.cfg
User,0,"45489940"
User,1,"47868650"
User,2,"52656727"
Res,0,"APPLDEV","RACFTST","RACF22"
Res,1,"BRLIMSYS","RACFPD","RACF22"
Res,2,"DEVELOP","RACFPD","RACF22"
Role,1001,"BASIC ROLE","Basic role - for all IT users","Enterprise","82922230","Org
Role","","45489940","Approved","09/05/2007 10:36","No Rule","Enterprise","Corporate",""
Role,1014,"Title - Product Manager","Characteristic Role (50%)","Title - Product Manager","99883135","Org
Role","","45489940","Approved","09/05/2007 10:36","Title=Product Manager","Title","Corporate",""
Role,1015,"Title - Operator","Characteristic Role (50%)","Title - Operator","45489940","Org
Role","","45489940","Approved","09/05/2007 10:36","Title=Operator","Title","Corporate",""
User-Res,0,2
User-Res,0,1
User-Role,1,1001
User-Role,2,1014
Role-Res,1001,0
Role-Res,1014,1
Role-Res,1014,2
Role-Role,1015,1014
Role-Role,1015,1001

```

Role Numbering

CA RCM provides automatic serial numbering of roles. If a configuration is created from an external source and roles are being imported, the Role Engineer can choose a specific numbering scheme, as long as the numbers are unique and the Role Name is unique.

Glossary

Approved Audit Card

An Audit Card where all the listed violations have been approved. It can be used during an audit to prevent repeated notices of violations that have already received approval.

Audit Card

A file with the extension .aud. It is generated by the DNA. It contains a list of violations or out of pattern situations. Each entry is a violation connected to an entity or to a link. It is possible to edit an Audit Card in the DNA module, adding instructions to either fix a violation or approve one. For further information see the DNA User Manual.

Children

Ticket-type specific.

The number of children listed for any campaign ticket denotes the number of Approvers assigned to the campaign.

The number of children listed for an Approver ticket is the number of [entities] the specific approver has to audit, where [entities] refers to the campaign type: user, role or resource certification.

Configuration

A CA RCM-proprietary data structure that holds a snapshot of the definitions of users, resources and roles (if available), as well as the relevant relationships (privileges) between them.

Connectors

Connectors use the converters to access the production computer for both download and upload processes. There are separate connectors for import and export procedures.

defaultSettings.xml

A connection details XML file located in the CA RCM home directory under the converter subdirectory. Use the CA RCM DM module to update.

Direct Link

An uninterrupted connection between two entities. For example: a user to resource link.

Dual Link

Refers to the case when both a direct link and an indirect link exist. For example: A user is linked directly to a specific resource, and at the same time the user is linked to a role that is linked to the same resource.

Entity

Refers to one of the following:

-
- User
 - Role
 - Resource

Indirect Link

A circuitous connection between two entities. For example: A user is linked to a specific role and the role is linked to a specific resource. The link between the user and the resource is an indirect link. Here are some further examples:

User—Role—Resource: Indirect link user to resource

User—Role—Role: Indirect link user to role (hierarchy)

User—Role—Role—Resource: Indirect link user to resource

Indirect links are not defined for the case of user to resource to role, where the user is linked directly to a resource and a role is linked directly to the same resource. The user in this case does not have any kind of link to the role in question.

Link or Entity Link

Refers to a connection between two entities. The possible links are:

- user-role
- user-resource
- role-resource
- role-role (hierarchy)

Links can be categorized as direct links, dual links or indirect links.

Mapping.xml

A mapping details XML file located in the <Eurekify home directory>\<Converter directory>. Use the Eurekify DM module to update.

Master-configuration

The original configuration downloaded from the production computer. The master-configuration presents the real-world definitions.

Model-configuration

A copy of the master-configuration. The audit process is run on the model-configuration and the resulting, updated set of configuration files is compared by the Eurekify Sage DNA system to the original, master-configuration files. The differences are then uploaded to the production computer.

RACI

A RACI diagram, or RACI matrix, is used to describe the roles and responsibilities of various teams or users. It is especially useful in clarifying roles and responsibilities in cross-functional/departmental projects and processes. Within the Eurekify Portal, this is the source of the Approvers mentioned in this manual. They are listed in the Accountable configuration file.

The RACI diagram divides tasks into four participatory responsibility types, which are then assigned to different roles in the project or process. The following responsibility types make up the acronym RACI:

Responsible

Those who do work to achieve the task. There can be multiple resources responsible.

Accountable

(Also Approver) The resource ultimately answerable for the correct and thorough completion of the task. There must be only one A resource specified for each task.

Consulted

Those whose opinions are sought. Two-way communication.

Informed

Those who are kept up-to-date on progress. One-way communication. Very often the role specified as "accountable" is also specified "responsible." Outside of this exception, it is generally recommended that each role in the project or process for each task receive at most one of the participatory role types. Although some companies and organizations do allow, for example, double participatory types, this generally implies that the roles have not yet been truly resolved and so impedes the value of the RACI approach in clarifying each role on each task. For further information on RACI see http://www.pmforum.org/library/tips/pdf_files/RACI_R_Web3_1.pdf.

Role to Role Link

This type of link represents a hierarchal relationship. Users who are members of a parent role are automatically members of the sub-role, and therefore provisioned with all the sub-roles privileges.

Ticket

Tickets are work items that can be viewed in the Ticket Queue. They can be work related or informational, and/or hierarchal, or provide a plain notification concerning a process.

Universe

A term used to denote a unique Master-configuration/Model-configuration pair.

Violations

A violation is a breach of corporate security policies, guidelines, BPRs and/or regulations. CA RCM identifies such infractions and lists them in Audit Cards, where relevant. While using the CA RCM Portal, you will come across Violations columns where relevant. The number listed in such columns provides the number of violations associated with the specific row in the table.

Workflow

Campaigns and approval processes are guided by a workflow, a collection of instructions that guide the application logic. The workflow is generated by Workpoint™, which is a Business Processes Management (BPM) workflow design engine.

Index

A

Accountable • 121, 132, 133, 135, 136, 137, 138, 229
Acknowledge • 23, 126, 205
Administration • 12, 17, 177, 178, 197, 214, 218, 224, 225, 228, 229, 230, 231, 261
Approval Process • 23, 34, 36, 37, 38, 121, 125, 126, 127, 128, 130, 131, 132, 133, 136, 137, 139, 140, 142, 143, 145, 147, 149, 150, 151, 152, 214
Approval Process Ticket • 34, 37, 38, 128
Approver • 17, 23, 34, 36, 121, 125, 128, 131, 132, 133, 135, 136, 139, 140, 141, 142, 144, 145, 146, 147, 150, 151, 152, 153, 229, 242, 261
Approver Ticket • 23, 121, 133, 139, 145, 147, 151, 261
Approver Ticket • 23
Approver Ticket • 23
Approver Ticket • 23
Approver Ticket • 121
Approver Ticket • 133
Approver Ticket • 139
Approver Ticket • 145
Approver Ticket • 147
Approver Ticket • 151
Approver Ticket • 261
Archive • 37, 38
Attachment • 33, 127, 131, 138, 141, 144, 146, 150, 153

B

BPR • 139

C

Campaign Ticket • 23, 32, 33, 261
Campaign Ticket • 23
Campaign Ticket • 23
Campaign Ticket • 32
Campaign Ticket • 33
Campaign Ticket • 261
Comment • 32, 37, 38, 127, 131, 138, 141, 144, 146, 150, 153
Connector • 21, 23, 178, 194, 197, 198, 201, 261

Consult • 23, 36, 121, 140, 141, 145, 146, 152, 153
Converter • 198, 201
Customize • 29

D

Delegate • 16, 38, 126, 130, 137, 140, 143, 145, 150, 152, 205, 242
DM client tool • 194, 198, 201
DNA client tool • 15, 21, 22, 74, 177, 194, 198, 201, 218, 228, 229, 242, 257

E

Email • 259
Entity Browser • 12, 261
Escalate • 37, 126, 130, 137, 140, 143, 145, 150, 152, 205, 242
Eurekify.cfg • 228, 242, 243
Export Connector • 22, 194, 197, 201

F

Filter • 16, 25, 29, 214, 224, 227, 242, 243, 244

G

Gfilter • 243

H

Home Page • 15, 16, 198, 201, 261

I

Import Connector • 19, 194, 197, 198
Info-ticket • 23, 31

M

Master • 19, 20, 22, 177, 178, 228, 257
Model • 19, 20, 22, 121, 177, 178, 257

P

Permissions • 17, 240
Properties • 17, 23, 32, 33, 34, 37, 38, 125, 128, 140, 145, 147, 152, 177, 224, 225, 226, 227, 261

R

RACI • 22, 121, 135, 177, 178, 228, 229, 230, 245, 261
Reassign • 259
Reports • 16, 261

S

Scheduler • 214, 261
Search • 25, 29
Security • 128, 135, 142
Self-Service • 12, 17, 23, 74, 121, 125, 128, 133, 135, 137, 138, 139, 140, 142, 143, 145, 147, 149, 150, 151, 152, 242
Severity • 198, 201
State • 27
Status • 25, 28, 37, 38

T

Ticket Queue • 12, 17, 23, 25, 29, 37, 38, 121, 126, 198, 201, 209, 231
TMS Administration • 231
Transaction Log • 34, 127, 131, 138, 141, 144, 146, 150, 153, 214

U

Universe • 12, 19, 20, 22, 121, 125, 142, 177, 178, 198, 201, 217, 228, 229, 230, 243, 257, 261