CA Role & Compliance Manager

Portal User Guide

r12.5 SP1

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

Contents

Chapter 5: Presenting the Home Page 49

Chapter 6: Tickets and the Ticket Queue 55

Chapter 7: Running Campaign-owner Tickets 77

Chapter 10: How to Use Dashboards 131

Chapter 11: Running Self-Service Tasks 135

Chapter 12: Role Definition Tickets 175

Chapter 17: Troubleshooting 293

Appendix A: CA RCM Properties 305

Appendix B: Portal Structure (XML) 307

Appendix C: CA RCM Configuration Data Formats 317

Glossary 321

Index 325

Chapter 1: Introduction

CA RCM software provides solutions for the design, implementation, ongoing management, and auditing of role-based privileges as well as solutions for the full enterprise compliance life cycle.

This manual 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 for CA RCM. The CA RCM Portal is designed to provide the user with access to the various Role Management (RM) and Compliance Management (CM) features, offered by the CA RCM system.

CA RCM targets one of the most sensitive areas in information security and computer infrastructure management: identity and access management (IAM) of user applications and enterprise role management (ERM). The large number of systems and applications and the frequent changes at large enterprises has made the management of authorization of employee access to information, applications and other resources a very complex task, especially given increasing regulatory requirements. CA RCM has developed an engine that aims to automatically align a procedure or person's access to his/her job at the enterprise. For in-depth details concerning the CA RCM architecture and technology see the documents *Data Management User Manual* and *DNA User Manual*.

The CA RCM Portal provides access to identity and access management (IAM) data that streamlines compliance and regulatory reporting. It also improves operational efficiency and provides corporate policy makers with increased clarity as to the enterprise risks. The CA RCM Portal provides on-the-fly access to campaign management, ticket management; business processes and entity information. These features helps customers clean up existing identity data and build a role model with the best available information. This model serves as the foundation to automate the user provisioning process and enhances identity life cycle management.

This section contains the following topics:

About This Guide

This guide describes CA RCM Portal operation and options.

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 285)

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 Management

Granting privileges; approval processes and certification campaigns are tracked via tickets. Tickets are issued when a campaign is generated, and also during the approval processes associated with the campaign. The user's Ticket Queue acts as a ticket "inbox" where the various tickets, including campaign tickets, notification tickets related to approval processes (whether campaign-related or following self-service requests), or other tickets generated by the system can be viewed and managed.

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 17)

Opening the CA RCM Portal

To open the CA RCM Portal

1. Run your browser.
2. Enter the address http://*ServerName*:*ServerPort*/eurekify and click Go.

   The Login screen opens.
3. Enter your User Name and Password in the text fields.

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

   The CA RCM Portal Home Page appears.

More information:

Using The CA RCM Portal Interface (see page 17)
Presenting the Home Page (see page 49)

Chapter 2: Using The CA RCM Portal Interface

This guide assumes that you are familiar with CA RCM DNA and Sage Data Manager modules and know how to access them to obtain required data, file names and locations and to generate necessary files. For more information, see the *DNA User Manual* and the *Data Management User Manual*.

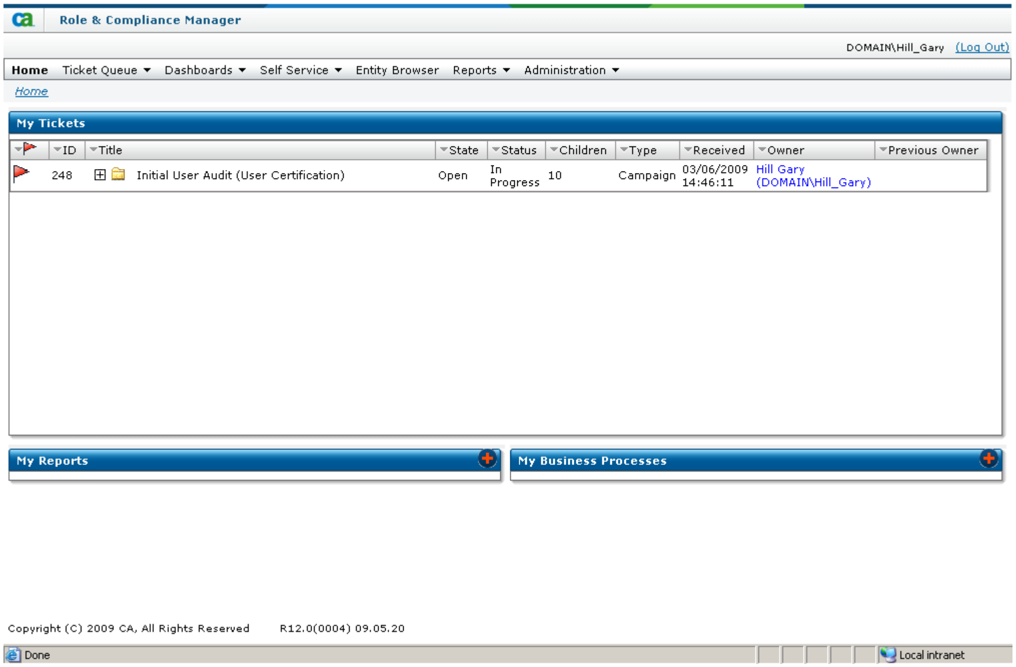
The user interface, menus and options are fully described in this chapter. Not all users will have full administrative privileges and therefore, not all the described options will be available for all users.

This section contains the following topics:

User Interface

To open the CA RCM Portal, follow the instructions in Opening the CA RCM Portal (see page 16).

The CA RCM Portal Home Page opens.



🚩	ID	Title	State	Status	Children	Type	Received	Owner	Previous Owner
🚩	248	⊞ Initial User Audit (User Certification)	Open	In Progress	10	Campaign	03/06/2009 14:46:11	Hill Gary (DOMAIN\Hill_Gary)	

Copyright (C) 2009 CA, All Rights Reserved R12.0(0004) 09.05.20

CA RCM Portal's home page contains the following main features: menu bar, Tickets pane, Reports navigation bar and Business Processes navigation bar. When the CA RCM Portal opens, the Tickets pane displays any active (new/open/done) tickets.

More information:

Presenting the Home Page (see page 49)

General Features

There are several features that repeat themselves in most of the screens you will access while working with the CA RCM Portal.

Autocomplete

Some of the Portal's screens have fields with an enabled Autocomplete feature. This feature provides a data list matching the field requirements from which you can make a selection.

To view the data list, press Down Arrow on your keyboard.

Mandatory Fields

Fields marked with an orange dot are mandatory. Attempting to go to the next stage of a process without filling in these fields causes an error message to be displayed next to each vacant field.

Data Table Features

When appropriate, the CA RCM Portal displays data in table format (data table). This is true for entity (for example, user, role, resource) data and for tickets that are generated as you work with the CA RCM Portal. There are several features that repeat themselves for most of the data tables that you access while working with the CA RCM Portal.

Customizing a Data Table

The Customize option is available for both Entity tables where it appears at the bottom of the data table and in the Ticket Queue (Customize). This option allows you to select which fields appear as columns in the data table.

To customize a data table

1. Click Customize.

   A Select Fields for <Entity> screen opens in a separate browser window.
2. In the Available Fields (left-hand) panel, select one or more (using Ctrl+Shift) of the listed fields.
3. Click the right arrow button to transfer the selected field(s) to the Selected Fields panel.
4. (Optional) To change the order of the fields listed in the Selected Fields panel select a field and click the down arrow or up arrow button.
5. To remove a field, from the Selected Fields panel, select the field and click the left arrow button.
6. When you finish making your selections, click OK.

   The selected fields will now appear in the relevant entity table.

Setting the Number of Records Per Page

Most Entity tables allow you to determine the number of records per page that you can view. The Records per page option appears at the bottom of the data table. This option allows you to select, from a pre-defined list, the number of records that will appear on every page. The default number of records per page for most data tables is 10.

Click the Records per page drop-down to specify the number of records displayed per page.

Filtering a Data Table

Entity information presented in table format can be filtered. When relevant, a Filter option appears at the bottom of the specific data table, or the filter statements will be part of the header of the screen displaying the entity table.

You can filter the table contents using a combination of criteria.

The filter allows only And statements. The filter 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 :

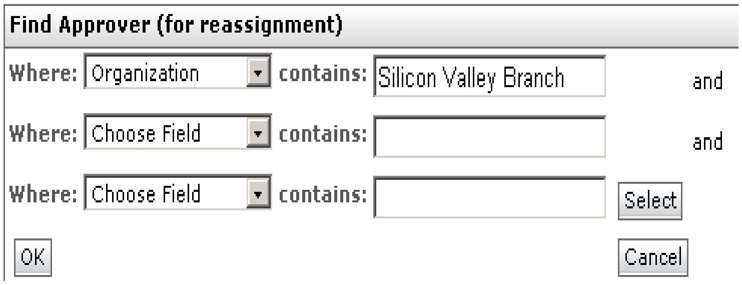
  [*Selected Field*] **Includes** [Free text]

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

To filter a data table

1. Click Filter.

   A Filter <Entity> screen opens in a separate browser window.



Find Approver (for reassignment)

Where: Organization contains: Silicon Valley Branch and

Where: Choose Field contains: and

Where: Choose Field contains:

2. Select the fields and their values from the drop-down lists. Enter text in the Includes box, if necessary.

   Note: The Autocomplete feature is active for the <Field Dependent Content> drop-down list. You can also start typing a value and the list will automatically scroll down to it.

3. Click OK.

   The current table will now be filtered according to the selections you made.

Entity Card and Data Table Tabs

The CA RCM Portal presents data in a very concise and easy to use manner. To facilitate this, the information is sometimes broken up into several parallel tables, and each table is located under a separate tab. For example, the Entity Browser shows the search results in three tables: Users, Roles and Resources, and each one is located under a separate tab. The active tab's label is bold, while the other tabs are gray.

Tabs can also be found in Entity Cards.

Click a tab label to bring that data table to the forefront (active). For example, if you click the RACI tab in a Role Card, the RACI table becomes active.

Sorting a Data Table by Column

The CA RCM Portal data tables can be sorted. When you click a column label, the table is sorted based on the selected column. Each type of data column has its own default presentation.

The Entity Card

You will come across entity lists (in table format), while using the CA RCM Portal. In most of these tables, one (or more) column(s) have active links, allowing you to view further information concerning a specific entity (user, role or resource). For example, when running the Self-Service option Manage my Team's Role Assignments, you can view a Users table. The content in the column showing the Person ID (user's ID) is highlighted. When you click on any specific Person ID, the specific user's card opens in a separate browser window.

The entity's card contains all the relevant information present within the selected Universe and includes lists of links (in table format) to the other entities. For example, in a User card, you have a Roles table and a Resources table. You can also access the cards belonging to linked entities by clicking on the relevant highlighted content from within a specific entity card.

These following options are available for all entity cards:

Customize

Allows you to customize this table.

Filter

Open a filter screen which you can use to filter the table contents.

Records per page

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

[Highlighted content in the entity card]

By clicking on specific content in the active column (usually this is the first column, the one that contains the user name/resource name), you can open the linked entity's data card.

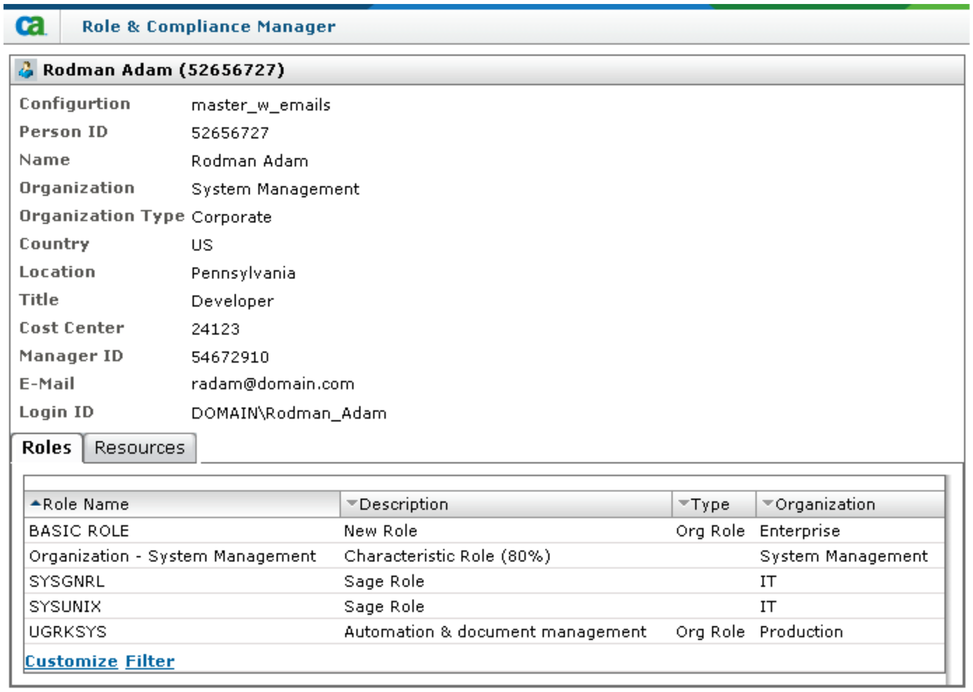
More information:

Customizing a Data Table (see page 19)
Setting the Number of Records Per Page (see page 20)

User Card

User cards present all the information concerning the specific user that is available in the selected Universe's configuration files. It also includes separate lists, under discrete tabs, of the user's linked Roles and Resources (in table format).

The User Card also includes separate lists (tabs), one for the user's linked Roles and one for the user's linked Resources as shown in the following screen:

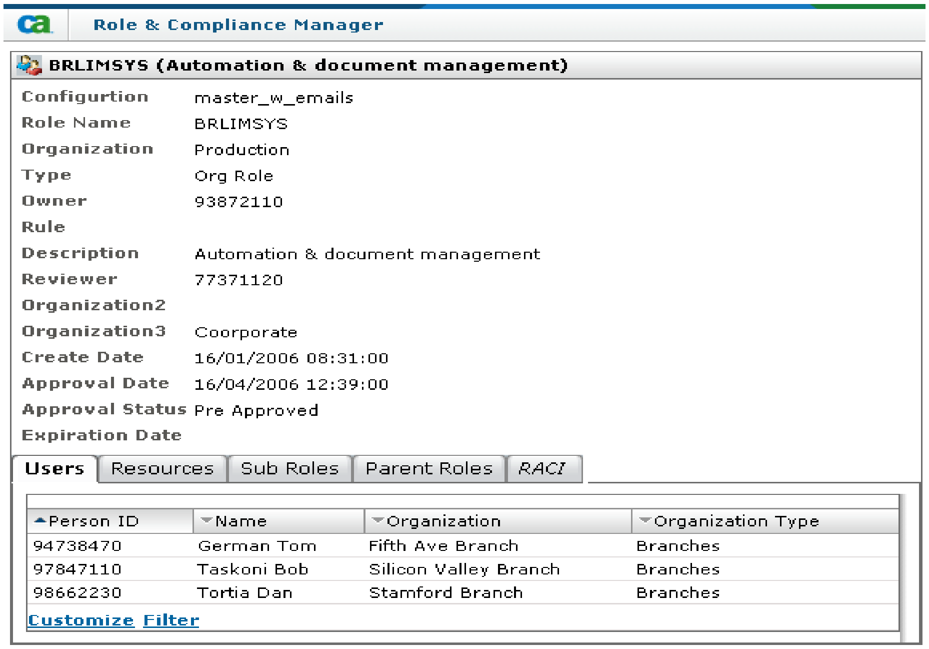


Configurtion	master_w_emails
Person ID	52656727
Name	Rodman Adam
Organization	System Management
Organization Type	Corporate
Country	US
Location	Pennsylvania
Title	Developer
Cost Center	24123
Manager ID	54672910
E-Mail	radam@domain.com
Login ID	DOMAIN\Rodman_Adam

Role Name	Description	Type	Organization
BASIC ROLE	New Role	Org Role	Enterprise
Organization - System Management	Characteristic Role (80%)		System Management
SYSGNRL	Sage Role		IT
SYSUNIX	Sage Role		IT
UGRKSYS	Automation & document management	Org Role	Production

Role Card

Role cards present all the information concerning the specific role that is available in the selected Universe's configuration files.



BRLIMSYS (Automation & document management)

Configurtion	master_w_emails
Role Name	BRLIMSYS
Organization	Production
Type	Org Role
Owner	93872110
Rule	
Description	Automation & document management
Reviewer	77371120
Organization2	
Organization3	Coorporate
Create Date	16/01/2006 08:31:00
Approval Date	16/04/2006 12:39:00
Approval Status	Pre Approved
Expiration Date	

Person ID	Name	Organization	Organization Type
94738470	German Tom	Fifth Ave Branch	Branches
97847110	Taskoni Bob	Silicon Valley Branch	Branches
98662230	Tortia Dan	Stamford Branch	Branches

The Role Card includes separate lists, under discrete tabs, of the following linked information (in table format):

Users

Provides a list of all the users linked to this role

Resources

Provides a list of all the resources linked to this role

Sub Roles

Provides a list of sub roles. This is a hierarchal link of the type role-to-role. Users who are members of the parent role (the current role) are automatically members of the sub-role (listed in this table) and therefore provisioned with all the sub-role's privileges.

Parent Role

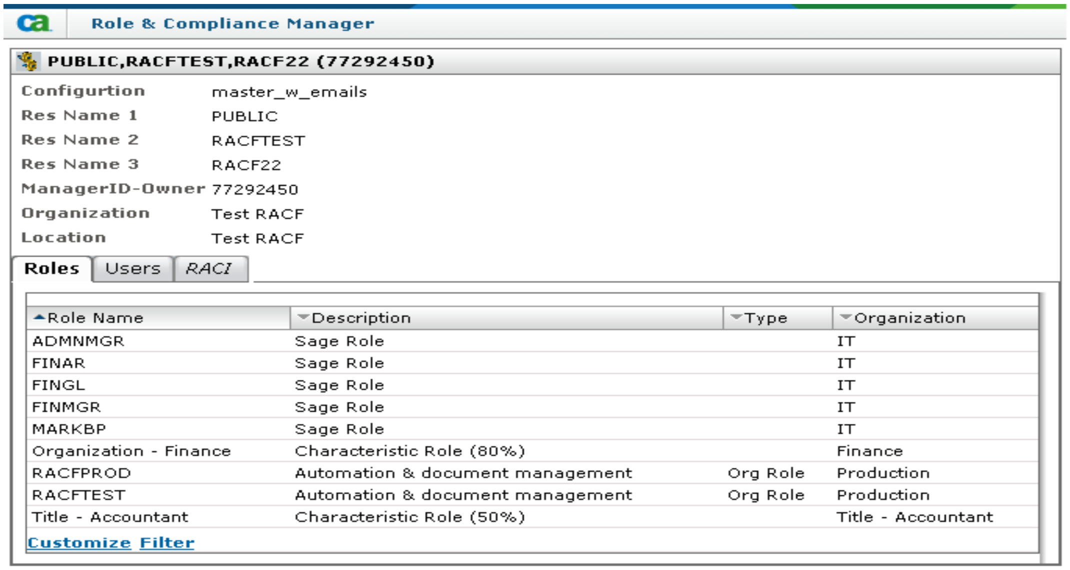
Provides a list of parent roles. This is a hierarchal link of the type role-to-role. Users who are members of the parent role (listed in this table) are automatically members of the sub-role (the current role) and therefore provisioned with all the sub-role's privileges.

RACI

Provides the name of the user who is Accountable for this role. This is the user who will be listed as the Approver when this role is being audited or when a change has been requested for this role.

Resource Card

Resource cards present all the information concerning the specific resource that is available in the selected Universe's configuration files.



PUBLIC,RACFTEST,RACF22 (77292450)

Configurtion	master_w_emails
Res Name 1	PUBLIC
Res Name 2	RACFTEST
Res Name 3	RACF22
ManagerID-Owner	77292450
Organization	Test RACF
Location	Test RACF

Role Name	Description	Type	Organization
ADMNMGR	Sage Role		IT
FINAR	Sage Role		IT
FINGL	Sage Role		IT
FINMGR	Sage Role		IT
MARKBP	Sage Role		IT
Organization - Finance	Characteristic Role (80%)		Finance
RACFPROD	Automation & document management	Org Role	Production
RACFTEST	Automation & document management	Org Role	Production
Title - Accountant	Characteristic Role (50%)		Title - Accountant

Resource cards also include separate lists, under discrete tabs, of the following linked information (in table format):

Roles

Provides a list of roles that are linked to this resource

Users

Provides a list of all the users linked to this resource

RACI

Provides the name of the user who is held accountable for this role. This is the user who will be listed as the Approver when this role is being audited or when a change has been requested for this role.

Menu Bar

The menu bar provides access to CA RCM Portal's functions. The menu bar is functionally organized and includes the following main items:

- Home
- Ticket Queue
- Dashboards
- Self-Service
- Entity Browser
- Reports
- Administration

Some of the menu bar items contain submenus with additional options. Where relevant, the name of the active window is indicated below the menu bar in italics.

Home

Click Home to return to the CA RCM Portal's home page.

More information:

Presenting the Home Page (see page 49)

Ticket Queue Menu

The Ticket Queue allows you to filter your tickets based on various criteria:

- Show the active ticket list. This includes tickets whose Status is Open, New or Done.
- Show the New Tickets list
- Show the Overdue Tickets list. Overdue tickets are flagged 🚩.
- Show the Approver Tickets list. This enables administrators to view all the Approver tickets associated with their own campaigns.
- Show the Campaign Tickets list. This option depends on the user's permissions.
- Show the Archived Tickets list.

More information:

Tickets and the Ticket Queue (see page 55)

Dashboards Menu

The dashboard automatically shows users useful information as they go about their tasks.

Self-Service Menu

The Self-Service menu provides access to a series of provisioning operations. Self-Service supports quick and easy user management by allowing the administrators/managers on-the-fly access to role and resource assignment requests for themselves and their team members. The Self-Service menu provides the following functions:

- Manage my team's role assignments
- Manage my role assignments
- Manage my team's resources' assignments
- Manage my resource assignments
- Request a new role definition
- Place a request to alter a role definition

More information:

Running Self-Service Tasks (see page 135)

Entity Browser

The Entity Browser opens the CA RCM Portal's Entity Browser Page. Here you can view information concerning Users, Roles or Resources for a selected Universe under a selected configuration.

The information is presented in three tables, where only one entity is visible at a time:

- Users table
- Roles table
- Resources table

More information:

Entity Browser (see page 209)

Reports Menu

The Reports menu provides access to the following families of reports

- Configuration reports
- Privileges quality management reports
- Role management reports
- Policy management reports
- Campaign Reports

Administration Menu

The Administration menu provides access to the following options:

- Add a campaign
- Job scheduling
- Accessing the TxLog page
- Load the cache
- Clear the cache
- Create RACI
- Synchronize RACI
- TMS administration
- Settings: Determine the settings for the Universe, Connectors and other basic properties:
- Connector Settings
- Universe Settings
- Properties Settings
- Common Properties Settings
- Audit Properties Settings
- Determine the CA RCM configuration settings
- System Checkup

More information:

Using Administration Functions (see page 221)

User Interface for Non-Administrators

The CA RCM Portal's flexibility becomes self-evident when examining the access it allows users with limited or no administrative rights. When such a user accesses the CA RCM Portal, the user can run any process and view any data for which he/she has been granted access permission. Available menu bar options will change according to the user's privileges.

For example, if you are a user (without administrative privileges) in charge of one or more resources, then when opening the CA RCM Portal you have a menu bar without the Administration option and the Self-Service menu is limited to viewing your personal roles and resources, and to handling the resources under your purview. The Ticket Queue allows access to Approver tickets that were allocated to you as a resource manager. Access to all other items via the menu bar would depend on your assigned permissions.

One of the advantages the CA RCM Portal gives its corporate users is that even individual users with very limited permissions, can still see tickets that are relevant to them. For example, a non-manager whose roles or resource access has been changed can view tickets informing him/her of these changes in his/her personal Ticket Queue. The following shows an example of a menu bar for a user with very limited permissions.

More information:

About Security & Permissions (see page 285)

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

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 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 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.

Dual links

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.

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 the completeness of the information, 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/or identity management system(s). 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 downloaded from the system (master) and the desired configuration generated following a campaign (model).

To create a Universe, you need the following information:

- Master configuration file name and path
- Model configuration file name and path
- Approved Audit Card (optional)
- Audit Settings file name and path (recommended)
- Names of the fields (in the configuration files) that contain the following information: login, email, user manager, role manager, and resource manager.

Note: You can provide names of configuration files that do not yet exist. In this case, you will not have the field names and you will have to create the master/model configuration files later and then update the Universe with the correct field names.

More information:

Setting a Universe (see page 235)

Step 2: Creating Import Connectors

After you have defined the universe that you intend to audit, you need to import the user and user privileges data from various end-points. This requires you to define import connectors.

Connectors allow you to import/export, for example, Active Directory, CSV, RACF or SQL files into the CA RCM, using a pre-defined converter, thereby creating a communications link to the downloading/uploading (production) server.

The connectors are defined as either import-connectors or export-connectors and utilize a specific pre-defined converter (see *Data Management User Guide*). “Import” refers to downloading the system’s true user, resource and role (when available) configuration data. “Export” refers to uploading the desired changes in user, resource and role data generated following an audit.

You will need the following information when you create a new connector:

- Name and location of the converter’s Settings XML file (see *Data Management User Manual*).
- Name and location of the converter’s Mapping XML file (see *Data Management User Manual*).
- (Optional) Name and location of the Enrichment Settings file (see *Data Management User Manual*).
- Name of the converter’s Java Class.
- Name of the Workflow process.

More information:

Setting Connectors to Import and Export Data (see page 239)

Step 3: Importing 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.

More information:

Monitor the First Run of a Connector (see page 248)

Step 4: Generating Master/Model Configurations

When you created the Universe, you provided the names of two configurations files: one was the master-configuration file and the other was the model-configuration file. The master configuration file contains the data imported from the system's endpoints. The model-configuration file is initially a copy of this data, which will be processed and updated as the role-modeling and audit processes proceed.

Use the instructions in Appendix A: Duplicating a Configuration (see page 303), to generate the master/model configuration files, using the CA RCM DNA module. If necessary, edit the Universe so that the listed master/model configurations will match the ones you generated.

After creating/editing a Universe, you have to enter the users associated with the universe into the CA RCM permisions configuration so that the users will have access to the CA RCM Portal. Typically this involves RACI synchronization to assign each user the rights they need on the portal.

More information:

CA RCM Configuration Settings (see page 274)
RACI Operations (see page 275)
Editing a Universe (see page 239)

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 the data they have to review and approve or reject, as the case may be.

More information:

Running a Campaign: A Case Study (see page 37)
Adding Campaigns (see page 222)

Step 6: Exporting Entity Data

The differences between the original “real-world” configuration that was downloaded from the system end-points (Master) and the updated and corrected configuration that has gone through an auditing process (Model) are uploaded 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 various regulations.

More information:

Creating a New Export Connector (see page 244)

Chapter 4: Showcasing the CA RCM Portal

Enterprise information security auditing has become increasingly relevant following new US and world-wide legislation mandating corporate and enterprise auditing. The computer security audit is a systematic, measurable technical assessment of how the confidentiality, availability and integrity of an organization's information is assured. CA RCM is capable of performing such security audits and it can also assist you in upgrading your information security.

The CA RCM Portal provides the Campaign facility as a tool towards assessing your corporate compliance with BPRs (Best Practice Rules) and the relevant legislation. It is recommended that you run campaigns regularly, on a quarterly or annual basis, though critical information systems, dealing with sensitive information or large monetary transactions, should probably be audited as often as once a month.

Running a Campaign

Campaigns review the system's permissions thereby assuring that only users with the appropriate provisioning can access the corporate resources, and that users who should not have access to various resources, are indeed barred from them. The CA RCM Portal campaign provides you with two basic options: either to approve the corporate permissions sent to you for review, or to reject them and notify the system that specific access permissions should be removed. The campaign does not check if users are lacking permissions that should have been granted to them.

Additional case studies can be found at: http://ca.com/support.

This section contains the following topics:

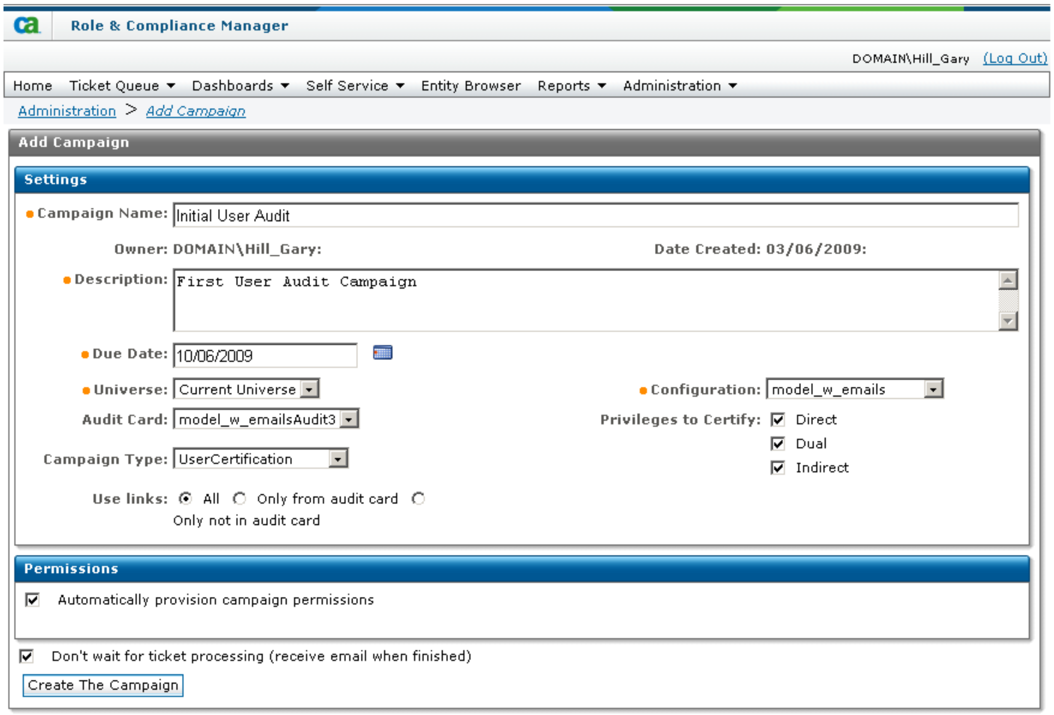
Running a Campaign: A Case Study

Gary Hill is a corporate branch manager, at the Silicon Valley branch. Gary must audit the company's information systems and validate correct usage of access rights to information resources.

The corporate system administrator has installed the CA RCM server and client modules and has downloaded the corporate security data, generating a set of CA RCM configuration files. Gary wants to use CA RCM to review the access rights of all users.

Defining a New User Campaign

Following the instructions for Adding Campaigns (see page 222), Gary defines the following campaign:


Role & Compliance Manager
DOMAIN\Hill_Gary (Log Out)
Home
Ticket Queue
Dashboards
Self Service
Entity Browser
Reports
Administration
Administration > Add Campaign

Add Campaign

Settings

Campaign Name: Initial User Audit

Owner: DOMAIN\Hill_Gary: Date Created: 03/06/2009:

Description: First User Audit Campaign

Due Date: 10/06/2009

Universe: Current Universe

Configuration: model_w_emails

Audit Card: model_w_emailsAudit3

Privileges to Certify: ☑ Direct ☑ Dual ☑ Indirect

Campaign Type: UserCertification

Use links: ● All ○ Only from audit card ○ Only not in audit card

Permissions

☑ Automatically provision campaign permissions

☑ Don't wait for ticket processing (receive email when finished)

Create The Campaign

Gary specifies the type or campaign and the data involved:

- He chooses the "universe" - the combination of users, role hierarchy, and resources that will form the basis for the campaign. He can also specify an Audit Card that includes analytical information relating to this universe.
- He also specifies the campaign type - campaigns can be focused on users, resources, or the role hierarchy itself.
- He selects the access privileges he wants to include for review. The campaign shown will include Direct and Indirect links between users and resources - and report situations where users and resources are linked by both direct and indirect links (Dual).

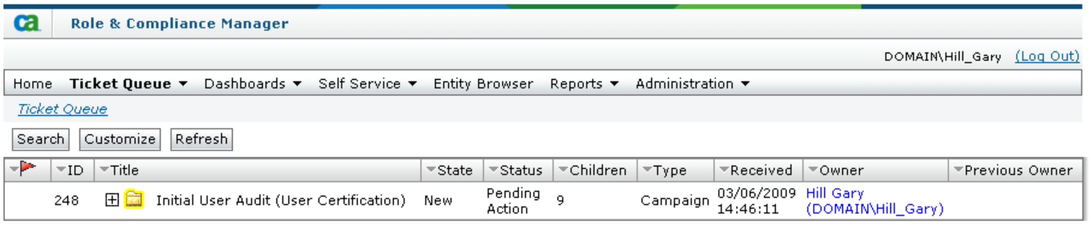
As the company is of moderate size, and setting up the campaign’s Approver tickets can take time, Gary chooses to run the campaign definition process in the background. The following message appears:

Campaign Requested

Your request was send for execution, an email message will be sent upon completion

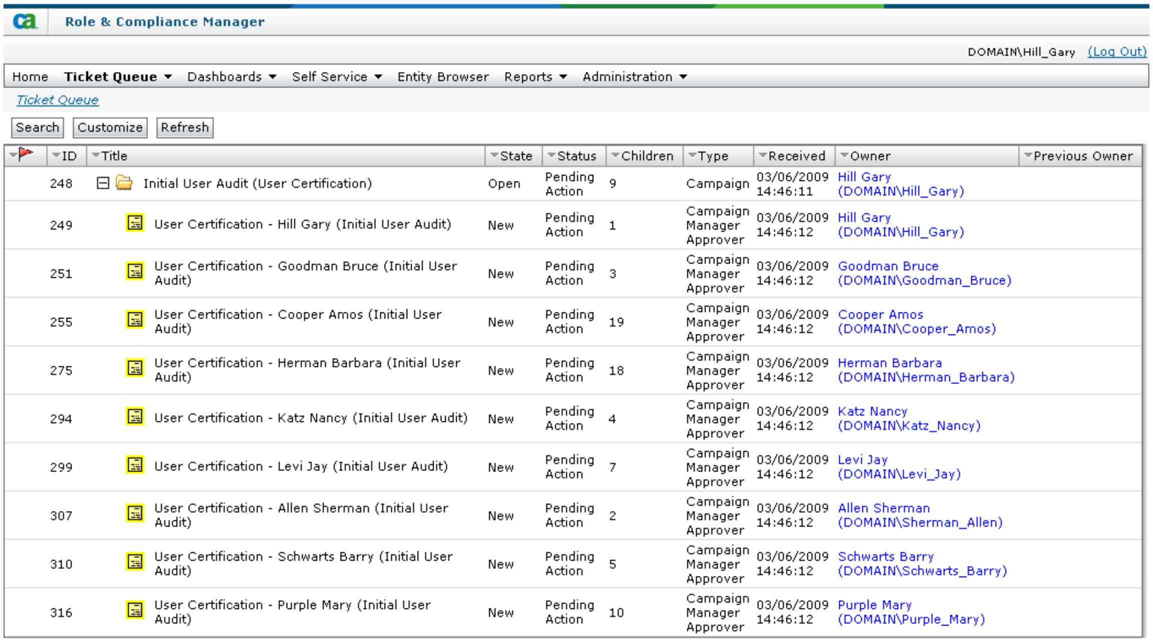
The CA RCM portal processes the user, role, and resource information in its active configuration. It generates review tasks for each manager of users or resources.

When the campaign is ready, the new user campaign's owner ticket appears in Gary's Ticket Queue when he logs in to the CA RCM portal.



ID	Title	State	Status	Children	Type	Received	Owner	Previous Owner
248	⊞ Initial User Audit (User Certification)	New	Pending Action	9	Campaign	03/06/2009 14:46:11	Hill Gary (DOMAIN\Hill_Gary)	

Under the Children column, the number 9 signifies that nine Approver tickets have been generated at this level in the reviewer tree - for Gary and the eight managers immediately under him in the reviewer tree:

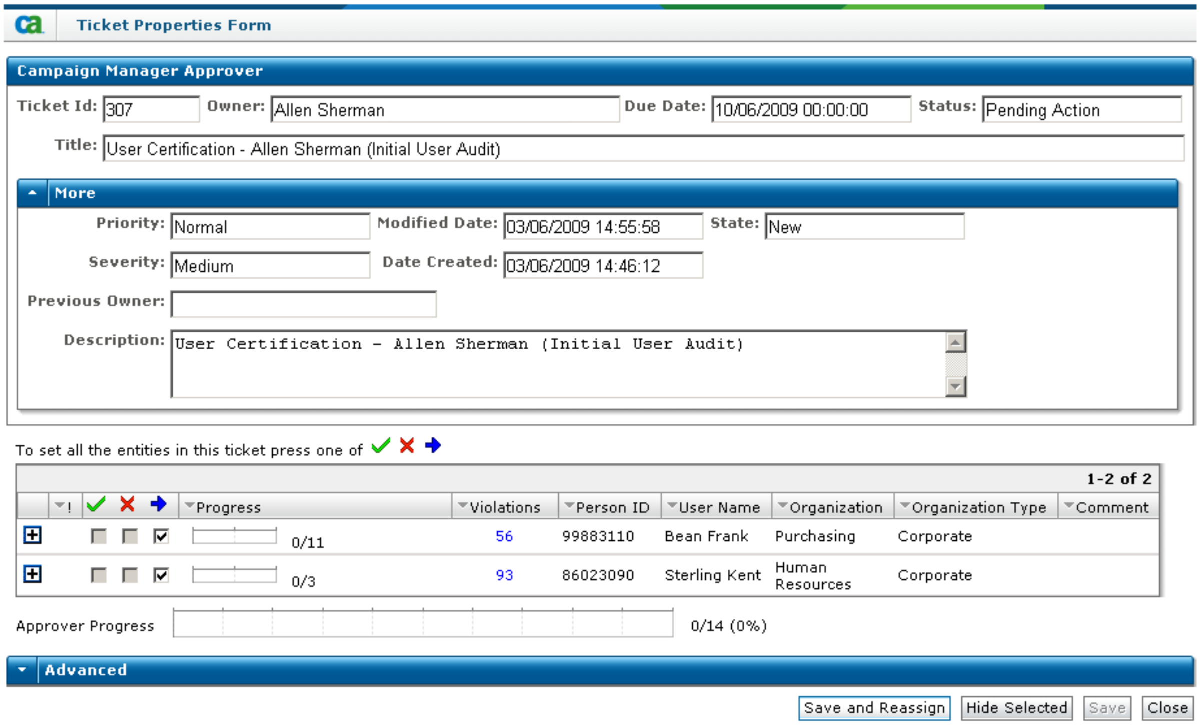


ID	Title	State	Status	Children	Type	Received	Owner	Previous Owner
248	⊟ Initial User Audit (User Certification)	Open	Pending Action	9	Campaign	03/06/2009 14:46:11	Hill Gary (DOMAIN\Hill_Gary)	
249	User Certification - Hill Gary (Initial User Audit)	New	Pending Action	1	Campaign Manager Approver	03/06/2009 14:46:12	Hill Gary (DOMAIN\Hill_Gary)	
251	User Certification - Goodman Bruce (Initial User Audit)	New	Pending Action	3	Campaign Manager Approver	03/06/2009 14:46:12	Goodman Bruce (DOMAIN\Goodman_Bruce)	
255	User Certification - Cooper Amos (Initial User Audit)	New	Pending Action	19	Campaign Manager Approver	03/06/2009 14:46:12	Cooper Amos (DOMAIN\Cooper_Amos)	
275	User Certification - Herman Barbara (Initial User Audit)	New	Pending Action	18	Campaign Manager Approver	03/06/2009 14:46:12	Herman Barbara (DOMAIN\Herman_Barbara)	
294	User Certification - Katz Nancy (Initial User Audit)	New	Pending Action	4	Campaign Manager Approver	03/06/2009 14:46:12	Katz Nancy (DOMAIN\Katz_Nancy)	
299	User Certification - Levi Jay (Initial User Audit)	New	Pending Action	7	Campaign Manager Approver	03/06/2009 14:46:12	Levi Jay (DOMAIN\Levi_Jay)	
307	User Certification - Allen Sherman (Initial User Audit)	New	Pending Action	2	Campaign Manager Approver	03/06/2009 14:46:12	Allen Sherman (DOMAIN\Sherman_Allen)	
310	User Certification - Schwarts Barry (Initial User Audit)	New	Pending Action	5	Campaign Manager Approver	03/06/2009 14:46:12	Schwarts Barry (DOMAIN\Schwarts_Barry)	
316	User Certification - Purple Mary (Initial User Audit)	New	Pending Action	10	Campaign Manager Approver	03/06/2009 14:46:12	Purple Mary (DOMAIN\Purple_Mary)	

The RACI (Responsible-Accountable-Consulted-Informed) information for the selected universe is used to set up the campaign's reviewer tree.

Reassigning Links to Another Approver

Reviewing the campaign Approvers, Gary finds that Allen Sherman is an approver - but Allen is on vacation. Gary decides to reassign the links in Allen's ticket to another approver.



Ticket Id: 307 Owner: Allen Sherman Due Date: 10/06/2009 00:00:00 Status: Pending Action

Title: User Certification - Allen Sherman (Initial User Audit)

Priority: Normal Modified Date: 03/06/2009 14:55:58 State: New

Severity: Medium Date Created: 03/06/2009 14:46:12

Previous Owner:

Description: User Certification - Allen Sherman (Initial User Audit)

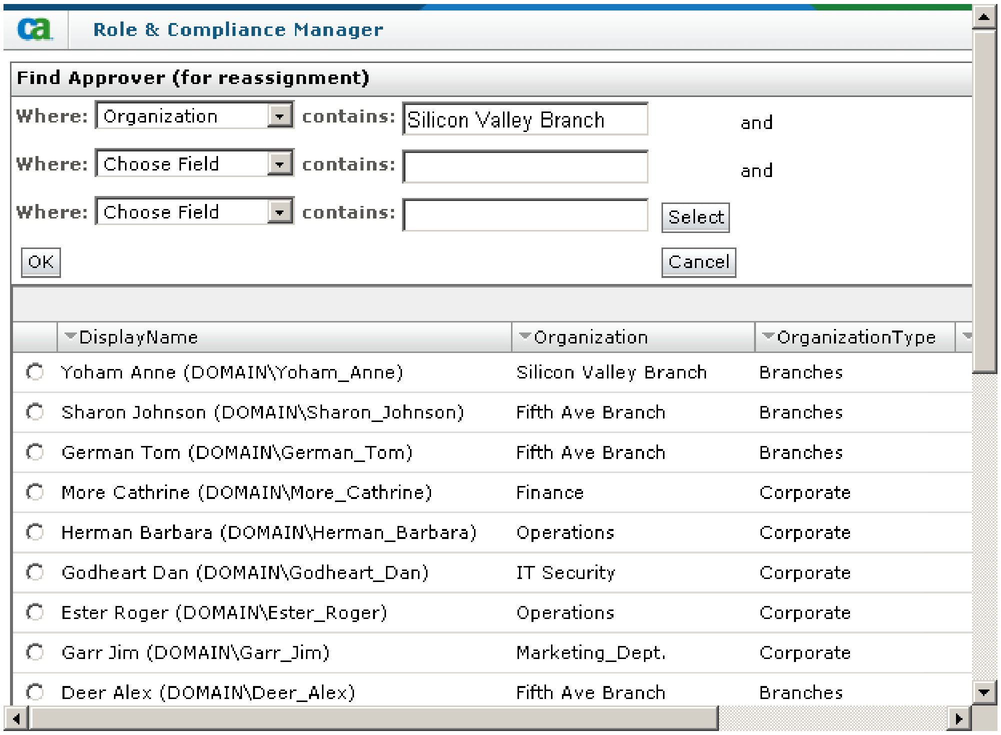
To set all the entities in this ticket press one of ✓ ✗ →

1-2 of 2

	!	✓	✗	→	Progress	Violations	Person ID	User Name	Organization	Organization Type	Comment
⊞		□	□	☑	0/11	56	99883110	Bean Frank	Purchasing	Corporate	
⊞		□	□	☑	0/3	93	86023090	Sterling Kent	Human Resources	Corporate	

Approver Progress 0/14 (0%)

Allen has two users listed in his ticket. He selects the Reassign (➡) check box located next to both users and clicks Save and Reassign. The Find Approver (for reassignment) screen opens.



Find Approver (for reassignment)

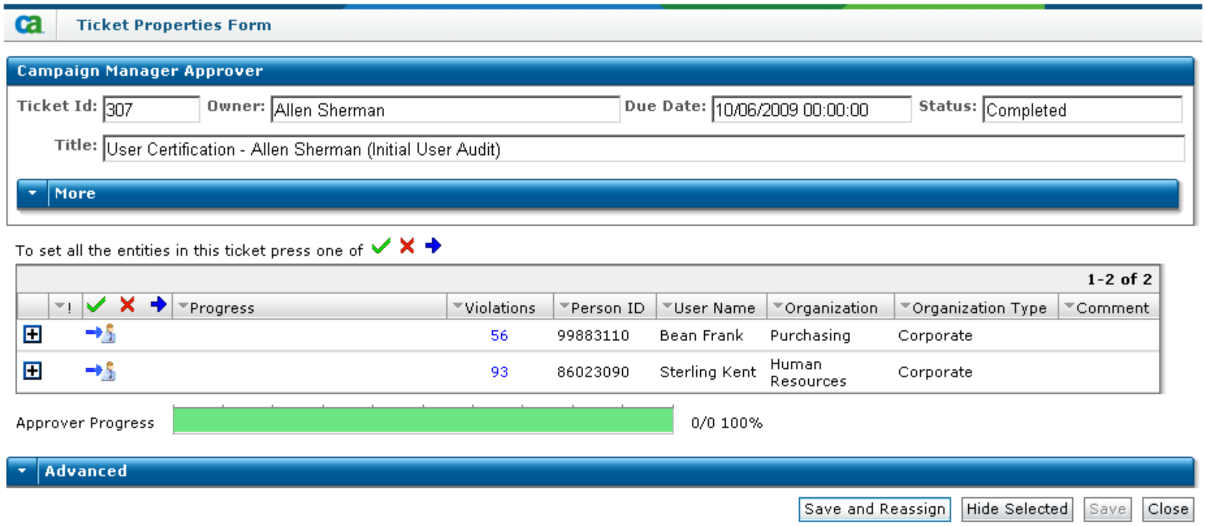
Where: Organization contains: Silicon Valley Branch and

Where: Choose Field contains: and

Where: Choose Field contains:

	DisplayName	Organization	OrganizationType
○	Yoham Anne (DOMAIN\Yoham_Anne)	Silicon Valley Branch	Branches
○	Sharon Johnson (DOMAIN\Sharon_Johnson)	Fifth Ave Branch	Branches
○	German Tom (DOMAIN\German_Tom)	Fifth Ave Branch	Branches
○	More Cathrine (DOMAIN\More_Cathrine)	Finance	Corporate
○	Herman Barbara (DOMAIN\Herman_Barbara)	Operations	Corporate
○	Godheart Dan (DOMAIN\Godheart_Dan)	IT Security	Corporate
○	Ester Roger (DOMAIN\Ester_Roger)	Operations	Corporate
○	Garr Jim (DOMAIN\Garr_Jim)	Marketing_Dept.	Corporate
○	Deer Alex (DOMAIN\Deer_Alex)	Fifth Ave Branch	Branches

To narrow down the number of users to choose from, Gary selects the filter Where Organization contains Silicon Valley Branch (the filter is case sensitive). For more information on using the filter options see Filtering a Data Table (see page 20). Gary reassigns Allen's users to Robert Mills.



Campaign Manager Approver

Ticket Id: 307 Owner: Allen Sherman Due Date: 10/06/2009 00:00:00 Status: Completed

Title: User Certification - Allen Sherman (Initial User Audit)

To set all the entities in this ticket press one of ✓ ✗ ➡

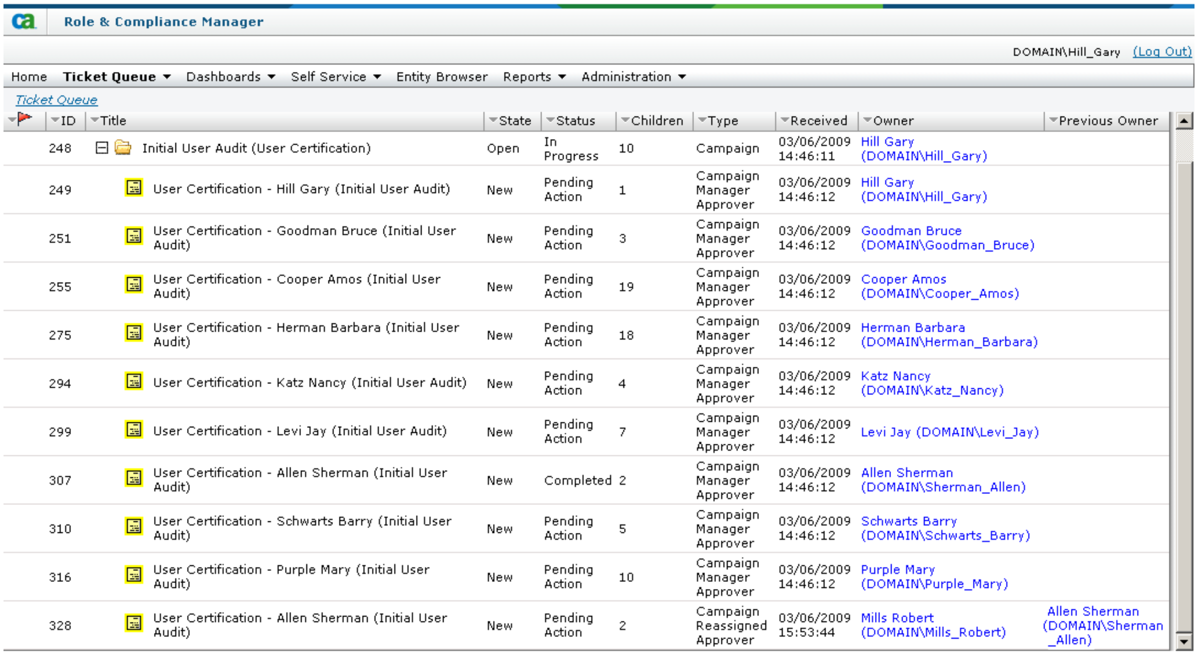
1-2 of 2

	!	✓	✗	➡	Progress	Violations	Person ID	User Name	Organization	Organization Type	Comment
⊞				➡		56	99883110	Bean Frank	Purchasing	Corporate	
⊞				➡		93	86023090	Sterling Kent	Human Resources	Corporate	

Approver Progress 0/0 100%

As all Allen's users have been reassigned, the Approver progress bar shows that the review process is 100% complete, and the users have a reassign icon (→) next to them.

In Gary’s Ticket Queue, Allen’s ticket now has the status Completed, and a new ticket has been generated for Robert Mills.



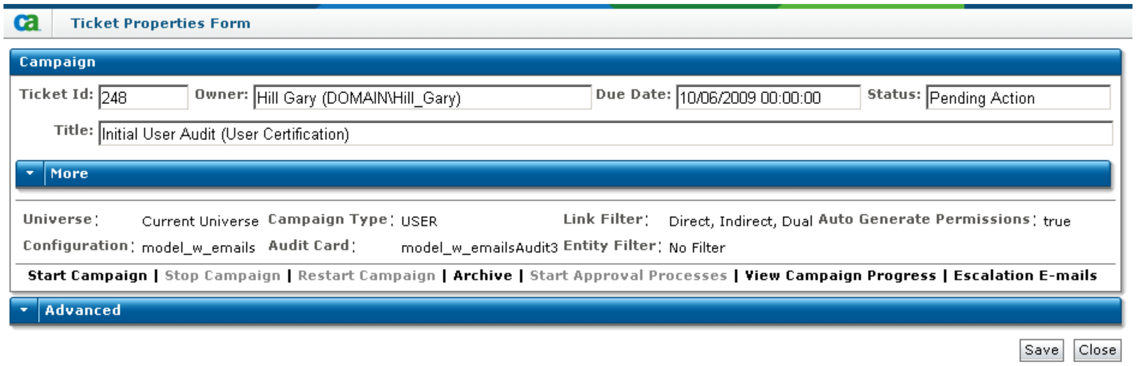
ID	Title	State	Status	Children	Type	Received	Owner	Previous Owner
248	Initial User Audit (User Certification)	Open	In Progress	10	Campaign	03/06/2009 14:46:11	Hill Gary (DOMAIN\Hill_Gary)	
249	User Certification - Hill Gary (Initial User Audit)	New	Pending Action	1	Campaign Manager Approver	03/06/2009 14:46:12	Hill Gary (DOMAIN\Hill_Gary)	
251	User Certification - Goodman Bruce (Initial User Audit)	New	Pending Action	3	Campaign Manager Approver	03/06/2009 14:46:12	Goodman Bruce (DOMAIN\Goodman_Bruce)	
255	User Certification - Cooper Amos (Initial User Audit)	New	Pending Action	19	Campaign Manager Approver	03/06/2009 14:46:12	Cooper Amos (DOMAIN\Cooper_Amos)	
275	User Certification - Herman Barbara (Initial User Audit)	New	Pending Action	18	Campaign Manager Approver	03/06/2009 14:46:12	Herman Barbara (DOMAIN\Herman_Barbara)	
294	User Certification - Katz Nancy (Initial User Audit)	New	Pending Action	4	Campaign Manager Approver	03/06/2009 14:46:12	Katz Nancy (DOMAIN\Katz_Nancy)	
299	User Certification - Levi Jay (Initial User Audit)	New	Pending Action	7	Campaign Manager Approver	03/06/2009 14:46:12	Levi Jay (DOMAIN\Levi_Jay)	
307	User Certification - Allen Sherman (Initial User Audit)	New	Completed	2	Campaign Manager Approver	03/06/2009 14:46:12	Allen Sherman (DOMAIN\Sherman_Allen)	
310	User Certification - Schwarts Barry (Initial User Audit)	New	Pending Action	5	Campaign Manager Approver	03/06/2009 14:46:12	Schwarts Barry (DOMAIN\Schwarts_Barry)	
316	User Certification - Purple Mary (Initial User Audit)	New	Pending Action	10	Campaign Manager Approver	03/06/2009 14:46:12	Purple Mary (DOMAIN\Purple_Mary)	
328	User Certification - Allen Sherman (Initial User Audit)	New	Pending Action	2	Campaign Reassigned Approver	03/06/2009 15:53:44	Mills Robert (DOMAIN\Mills_Robert)	Allen Sherman (DOMAIN\Sherman_Allen)

More information:

Campaign Approver Tickets (see page 95)
Reassigning a Link (see page 100)

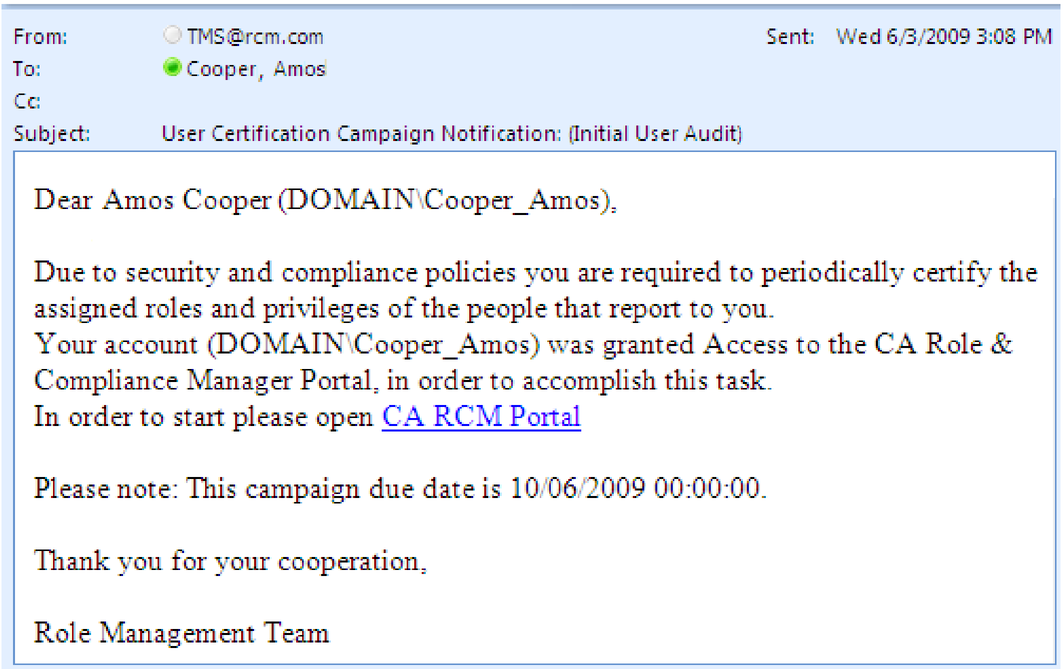
Starting the User Campaign

After checking approver assignments, Gary opens his campaign-owner ticket.


Ticket Properties Form
Campaign
More
Start Campaign | Stop Campaign | Restart Campaign | Archive | Start Approval Processes | View Campaign Progress | Escalation E-mails
Advanced
Save
Close

Ticket Id:	248	Owner:	Hill Gary (DOMAIN\Hill_Gary)	Due Date:	10/06/2009 00:00:00	Status:	Pending Action
Title:	Initial User Audit (User Certification)						
Universe:	Current Universe	Campaign Type:	USER	Link Filter:	Direct, Indirect, Dual	Auto Generate Permissions:	true
Configuration:	model_w_emails	Audit Card:	model_w_emailsAudit3	Entity Filter:	No Filter		

To start the campaign, Gary clicks Start Campaign. Emails are sent to all approvers, and tickets relating to this campaign are now visible to them when they log in to the CA RCM portal.



From: TMS@rcm.com Sent: Wed 6/3/2009 3:08 PM
To: Cooper, Amos
Cc:
Subject: User Certification Campaign Notification: (Initial User Audit)

Dear Amos Cooper (DOMAIN\Cooper_Amos),

Due to security and compliance policies you are required to periodically certify the assigned roles and privileges of the people that report to you.
Your account (DOMAIN\Cooper_Amos) was granted Access to the CA Role & Compliance Manager Portal, in order to accomplish this task.
In order to start please open CA RCM Portal

Please note: This campaign due date is 10/06/2009 00:00:00.

Thank you for your cooperation,

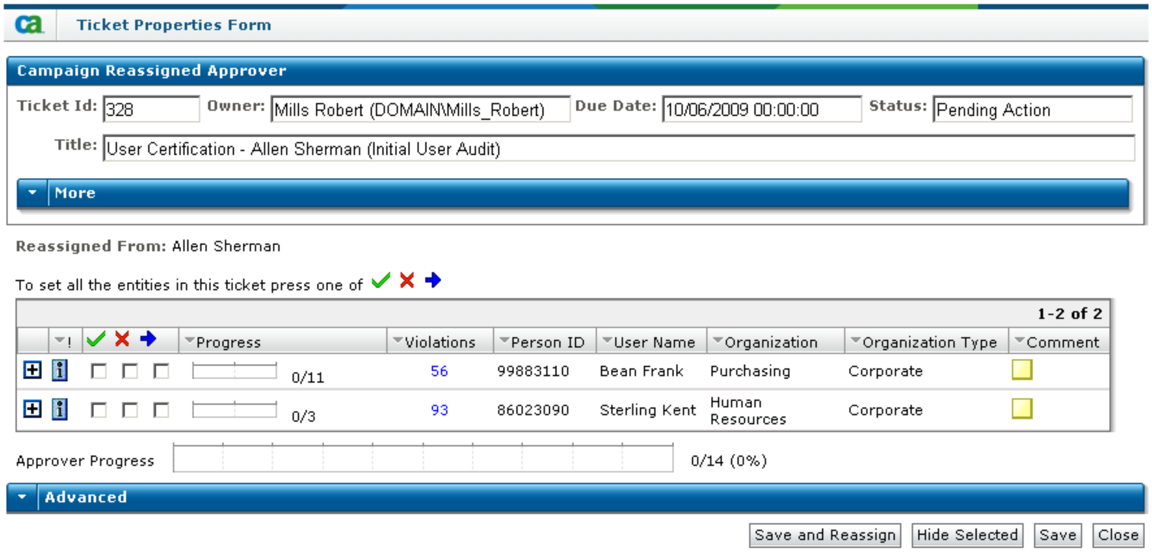
Role Management Team

More information:

Running Campaign-owner Tickets (see page 77)

Examining a User's Links

When Robert Mills receives his email, he logs in to the CA RCM portal. An approver's ticket is waiting in his Ticket Queue. It shows the review tasks he must perform as part of the campaign.



Ticket Properties Form

Campaign Reassigned Approver

Ticket Id:	328	Owner:	Mills Robert (DOMAIN\Mills_Robert)	Due Date:	10/06/2009 00:00:00	Status:	Pending Action
Title:	User Certification - Allen Sherman (Initial User Audit)						

More

Reassigned From: Allen Sherman

To set all the entities in this ticket press one of ✓ ✗ →

1-2 of 2

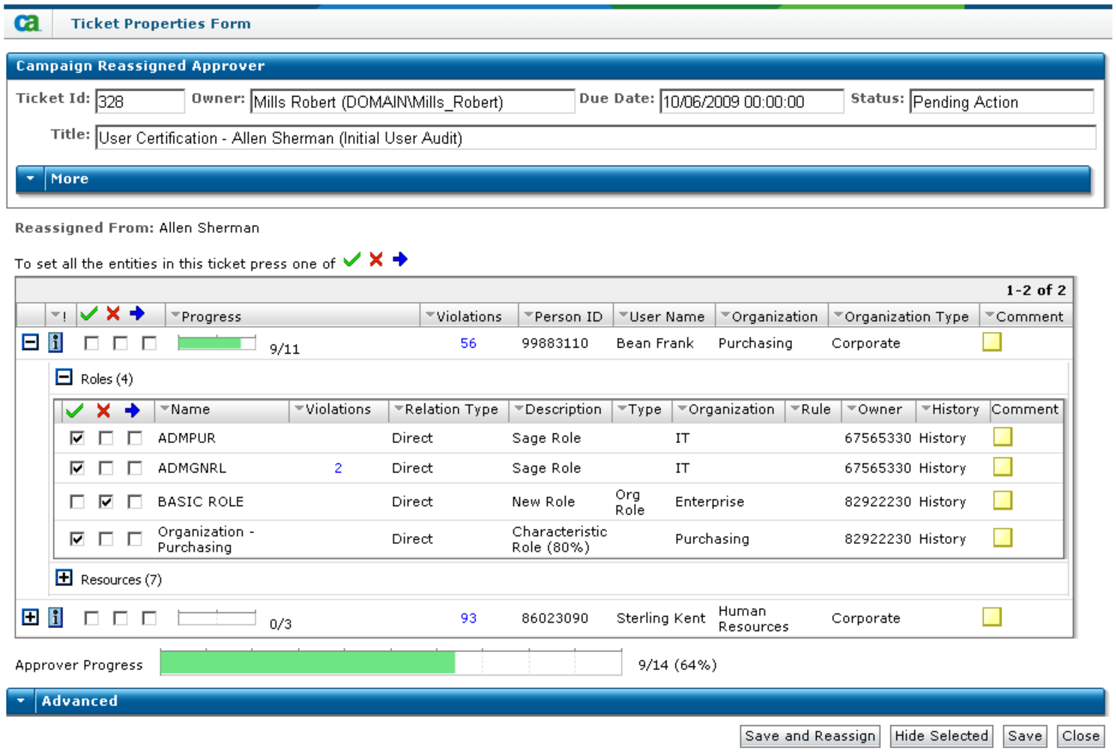
	!	✓	✗	→	Progress	Violations	Person ID	User Name	Organization	Organization Type	Comment
⊞	ℹ	□	□	□	0/11	56	99883110	Bean Frank	Purchasing	Corporate	🟨
⊞	ℹ	□	□	□	0/3	93	86023090	Sterling Kent	Human Resources	Corporate	🟨

Approver Progress 0/14 (0%)

Advanced

In this case, the ticket shows the two users that were originally assigned to Allen Sherman.

To see further details about the links to be reviewed, Robert expands the sections of the ticket.



Campaign Reassigned Approver

Ticket Id: 328 **Owner:** Mills Robert (DOMAIN\Mills_Robert) **Due Date:** 10/06/2009 00:00:00 **Status:** Pending Action

Title: User Certification - Allen Sherman (Initial User Audit)

Reassigned From: Allen Sherman

To set all the entities in this ticket press one of ✓ ✗ →

1-2 of 2

	!	✓	✗	→	Progress	Violations	Person ID	User Name	Organization	Organization Type	Comment
⊟	i	□	□	□	9/11	56	99883110	Bean Frank	Purchasing	Corporate	□
⊞	i	□	□	□	0/3	93	86023090	Sterling Kent	Human Resources	Corporate	□

⊟ Roles (4)

✓	✗	→	Name	Violations	Relation Type	Description	Type	Organization	Rule	Owner	History	Comment
☑	□	□	ADMPUR		Direct	Sage Role		IT		67565330	History	□
☑	□	□	ADMGNRL	2	Direct	Sage Role		IT		67565330	History	□
□	☑	□	BASIC ROLE		Direct	New Role	Org Role	Enterprise		82922230	History	□
☑	□	□	Organization - Purchasing		Direct	Characteristic Role (80%)		Purchasing		82922230	History	□

⊞ Resources (7)

Approver Progress 9/14 (64%)

Following the instructions found in Campaign Approver Tickets *(see page 95)*, Robert approves or rejects the various links.

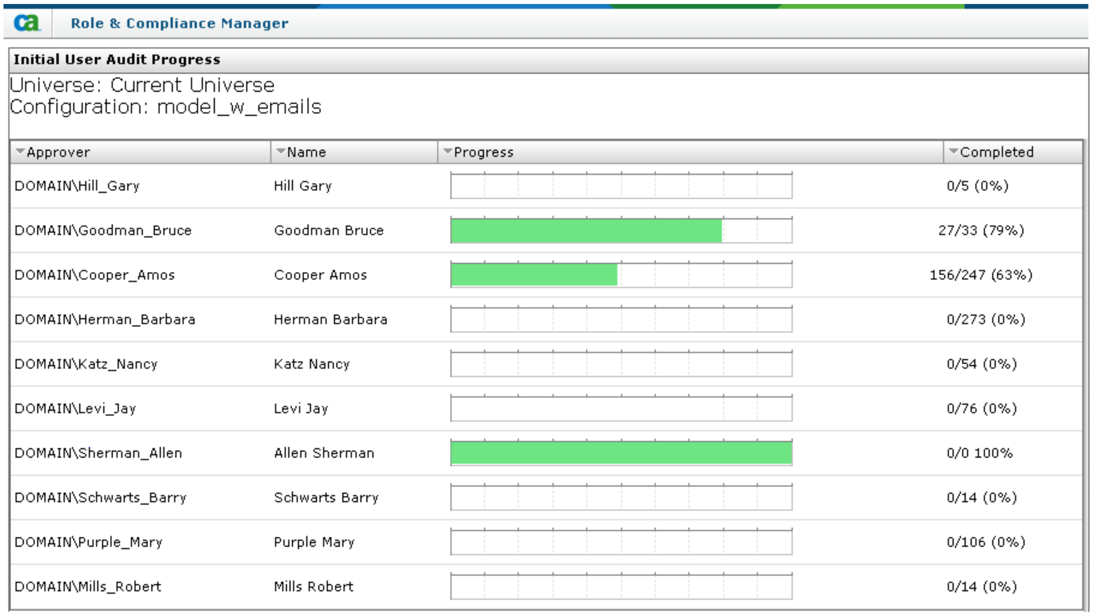
More information:

Campaign Approver Tickets (see page 95)

Checking the Campaign's Progress

As a campaign owner Gary monitors the progress of the approvers and makes sure that they are aware of the campaign’s deadline. To check on the campaign’s progress, Gary clicks the View Campaign Progress button located in the campaign-owner’s ticket.

The campaign progress screen opens in a separate browser window.



Initial User Audit Progress

Universe: Current Universe
Configuration: model_w_emails

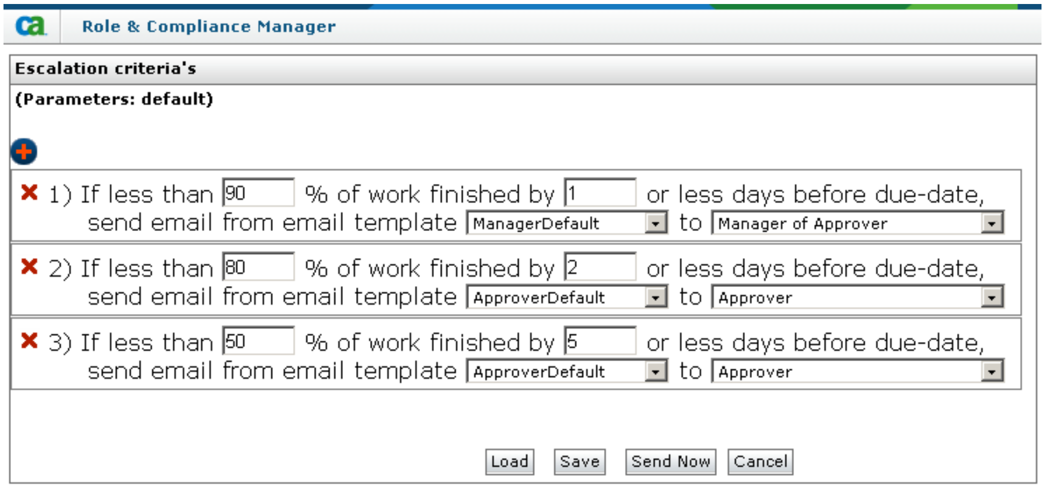
Approver	Name	Progress	Completed
DOMAIN\Hill_Gary	Hill Gary		0/5 (0%)
DOMAIN\Goodman_Bruce	Goodman Bruce		27/33 (79%)
DOMAIN\Cooper_Amos	Cooper Amos		156/247 (63%)
DOMAIN\Herman_Barbara	Herman Barbara		0/273 (0%)
DOMAIN\Katz_Nancy	Katz Nancy		0/54 (0%)
DOMAIN\Levi_Jay	Levi Jay		0/76 (0%)
DOMAIN\Sherman_Allen	Allen Sherman		0/0 100%
DOMAIN\Schwarts_Barry	Schwarts Barry		0/14 (0%)
DOMAIN\Purple_Mary	Purple Mary		0/106 (0%)
DOMAIN\Mills_Robert	Mills Robert		0/14 (0%)

More information:

View Campaign Progress (see page 91)

Sending Reminders to Approvers

As the campaign's due date nears, Gary sends reminders to the Approvers who have not yet finished reviewing their Approver tickets. In the campaign-owner ticket, he clicks Send Reminder. The Send Reminder screen opens in a separate browser screen.



Escalation criteria's

(Parameters: default)

✕ 1) If less than 90 % of work finished by 1 or less days before due-date, send email from email template ManagerDefault to Manager of Approver

✕ 2) If less than 80 % of work finished by 2 or less days before due-date, send email from email template ApproverDefault to Approver

✕ 3) If less than 50 % of work finished by 5 or less days before due-date, send email from email template ApproverDefault to Approver

Gary configures the completion thresholds and email texts that he wishes to send to approvers at various stages of the campaign.

Starting the Approval Process

When all the approvers have approved or rejected the links assigned to them, or when the campaign is manually ended, Gary can start the Approval Process. The Approval Process reviews the links rejected during the campaign.

While the initial campaign focused on one entity (user, role or resource), in the Approval Process administrators responsible for each end of the link must review and approve the change. For example, if a user—role link is rejected, then the relevant user manager and the relevant role manager will receive tickets as part of the Approval Process. Only if both managers agree to reject the link will the link be severed within the role hierachy's configuration files.

To start the Approval Process, Gary clicks Start Approval Process in his campaign owner ticket.

The CA RCM Portal generates the Approval Process tickets and sends email notifications to managers who must approve changes.

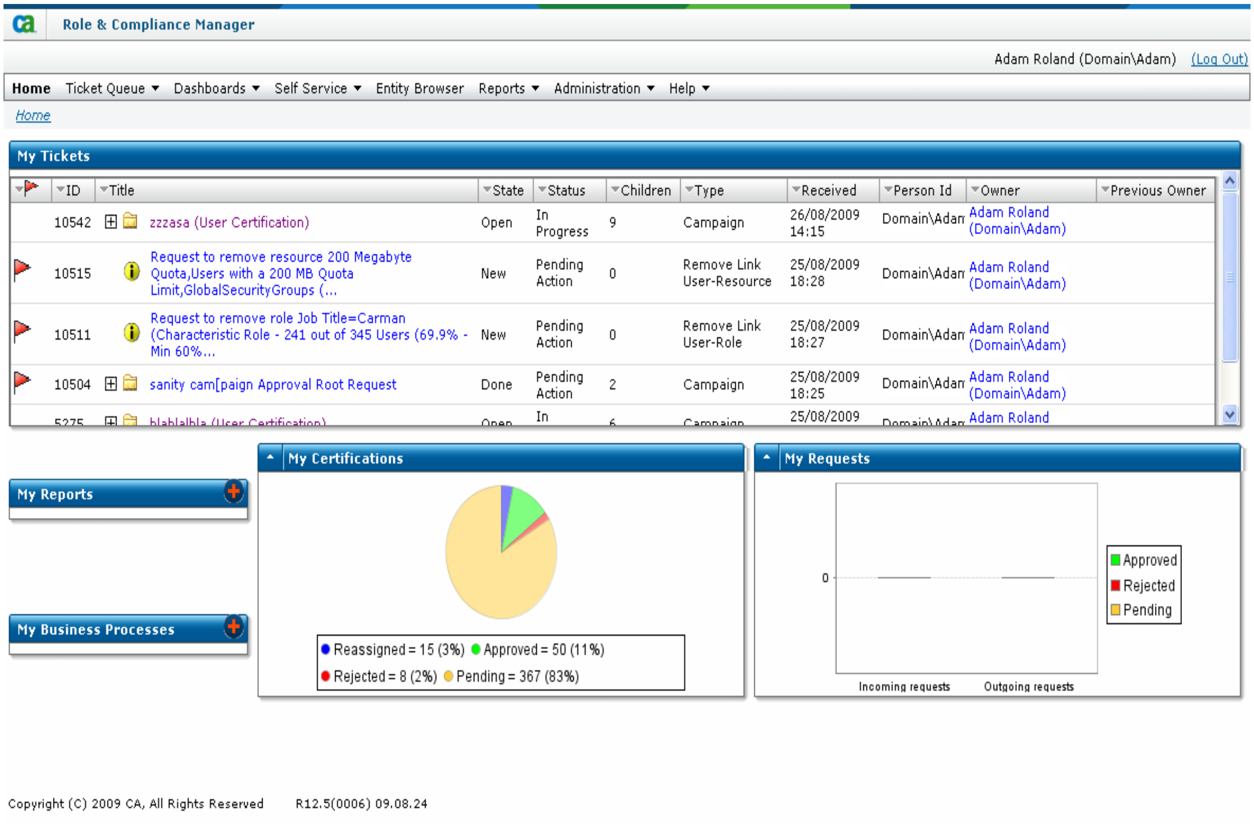
Following the Approval Process, a user may find that roles or resources that were once available are no longer accessible. If the user needs those resources to perform his/her tasks, they can ask their manager to reassign the relevant roles or resources.

More information:

Approval Process Tickets (see page 105)
Running Self-Service Tasks (see page 135)

Chapter 5: Presenting the Home Page

The CA RCM Portal’s home page displays your currently active tickets and provides easy access to your most frequently used reports and business processes.



	ID		Title	State	Status	Children	Type	Received	Person Id	Owner	Previous Owner
	10542	⊞	zzzasa (User Certification)	Open	In Progress	9	Campaign	26/08/2009 14:15	Domain\Adam	Adam Roland (Domain\Adam)	
🚩	10515	ⓘ	Request to remove resource 200 Megabyte Quota,Users with a 200 MB Quota Limit,GlobalSecurityGroups (...	New	Pending Action	0	Remove Link User-Resource	25/08/2009 18:28	Domain\Adam	Adam Roland (Domain\Adam)	
🚩	10511	ⓘ	Request to remove role Job Title=Carman (Characteristic Role - 241 out of 345 Users (69.9% - Min 60%...	New	Pending Action	0	Remove Link User-Role	25/08/2009 18:27	Domain\Adam	Adam Roland (Domain\Adam)	
🚩	10504	⊞	sanity cam[paign Approval Root Request	Done	Pending Action	2	Campaign	25/08/2009 18:25	Domain\Adam	Adam Roland (Domain\Adam)	
	5275	⊞	blahlalbla (User Certification)	Open	In	6	Campaign	25/08/2009	Domain\Adam	Adam Roland	

Copyright (C) 2009 CA, All Rights Reserved R12.5(0006) 09.08.24

This section contains the following topics:

The Tickets Pane (see page 50)
The Reports Bar (see page 51)
The Business Processes Bar (see page 52)
The Certifications Bar (see page 52)
The Requests Bar (see page 53)

The Tickets Pane

This panel provides you with a table containing a list of your tickets. The tickets displayed in this pane are campaign-owner tickets for the campaigns you have created; campaign-Approver tickets when you are an approver for a specific campaign; Approver tickets for entities you were assigned to manage and info-tickets. Some of the tickets have hierarchal tree structures that you can navigate. The type of data (fields) displayed in this pane is determined by customizing the Ticket Queue. Each column can be used to sort the ticket table. Highlighted content displayed in the panel enables you to link to additional data.

You can navigate the tickets by clicking on ⊞. Clicking an active link in the Title column opens the Ticket Properties Form in a separate browser window. Clicking on the link in the Owner column will open the listed ticket owner's User Card in a separate browser window.

The following table presents the icons used in the Ticket pane and their description:

Icon	Description
📁	New ticket folder
📁	Ticket folder. This is a task ticket that has children tickets. The ticket tree headed by this folder could have been generated when this ticket was first generated, or later in the process.
ℹ	New info-ticket
ℹ	Info-ticket
📋	New task ticket
📋	Task. This icon appears next to every ticket that refers to an action.
🚩	Overdue ticket
✖	Appears when a ticket refers to a process that includes errors.
⊞	Click to expand the ticket tree
⊟	Click to collapse the ticket tree

More information:

Tickets and the Ticket Queue (see page 55)
Running Campaign-owner Tickets (see page 77)
Campaign Approver Tickets (see page 95)

The Reports Bar

The Reports navigation bar lets you easily navigate to your most popular reports. Click ⊕ to add links to your favorite reports.

To add a report link to the list of reports displayed in the Reports Pane

1. In the Reports bar header click ⊕.

   The Select Links for My Reports screen opens in a separate browser window.

2. In the Available Links (left-hand) panel, select one or more (using Ctrl/Shift) of the report links.

3. Click → to transfer the selected link(s) to the Selected Links pane.

4. (Optional) To change the order of the listed links in the Selected Links pane select a link and click ↓ or ↑.

5. To remove a report link from the Selected Links pane select the link and click ←.

6. When you finish making your selections, click OK.

   The selected links will now appear in the Home page Reports navigation bar.

The Business Processes Bar

The Business Processes navigation bar lets you easily navigate to your most popular business processes. The business processes that are available from the bar are also listed in the Self-Service menu.

You can click ⊕ to add links to your favorite ones.

To generate a list of Business Process links

1. In the Business Process navigation bar header click ⊕.

   The Select Links for Business Process screen opens in a separate browser window.

2. In the Available Links (left-hand) panel, select one or more (using Ctrl/Shift) of the business process links.
3. Click → to transfer the selected link(s) to the Selected Links pane.
4. (Optional) To change the order of the listed links in the Selected Links pane select a link and click ↓ or ↑.
5. To remove a business process link from the Selected Links pane select the link and click ←.
6. When you have finished making your selections, click OK.

   The selected links appear in the Home page Business Processes navigation bar.

More information:

Running Self-Service Tasks (see page 135)

The Certifications Bar

This chart provides up-to-date information about your campaigns. Any campaign in which you are an approver and need to approve, reject, or reassign entities or links appears. The chart provides quick overview of the completed rejected, approved, and pending certification tasks.

The chart displays a count of tickets that belong to campaigns with status of pending action, rejected, approved and reassigned.

You can hide the chart by clicking the upper left icon. CA RCM remembers your selection.

If no chart data is available, the "You are not assigned to any campaign" message appears.

The Requests Bar

The requests panel provides an up to date view of your self-service approval requests.

The chart has two bars:

Incoming Requests

Displays the number of requests that others issued and you need to approve or reject.

Outgoing Requests

Displays the number of requests that you made using the self service options that others need to approve or reject.

The charts count tickets that belong to the self service operation that you made or that you should approve or reject.

Both bar charts count approved, rejected, and pending tickets of self service operations that are not archived. When you approve or reject, your Incoming bar counter increments. When one of your requests is approved or rejected your Outgoing bar increments. When the initiator acknowledges the base ticket, all the tickets under it are not counted anymore.

Chapter 6: Tickets and the Ticket Queue

Tickets have a unique place in the CA RCM. CA RCM Portal tickets are work items and they are used to transfer data, run campaigns, certify roles, update privileges and more. The Ticket Queue menu provides a series of filtered display options allowing you to view filtered lists of tickets (in table format) in the Ticket Queue window. The available filtering options provided by the Ticket Queue menu are:

- Open/New/Done Tickets
- New Tickets
- Over Due
- Approver Tickets
- Campaign Tickets
- Archived Tickets

Administrators can see their own tickets, and also tickets assigned to their team(s), campaign tickets that are associated with campaigns they created and approval process tickets associated with the same campaigns. Other users, who do not have administration rights, can see only their own tickets (where they are listed as the ticket Owner).

Specific ticket data and functionality can be accessed by clicking on a specific ticket and opening its Ticket Properties Form in a separate browser window. The data, functions and options available to the user from within a Ticket Properties Form depends on the ticket type.

Tickets, in general, encompass two types of functions:

- Link related actions
- Ticket related actions

Link related actions can be found in the Campaign Approver tickets.

Ticket related actions depend on the ticket type. Ticket functionality includes general functions, such as Close or Save, that are generic for all ticket types, and specialty functions that are available for specific types of tickets, such as the View Campaign Progress option, which is unique to campaign-owner tickets, or Acknowledge, which is found in info-tickets.

This section contains the following topics:

Ticket Life Cycle

The ticket's purpose and functionality governs its life cycle. A ticket life cycle can be very simple or extremely complex. You can gain information on a specific ticket's current situation by checking the fields State and Status, either in the Ticket Queue table (see page 62), or in the Ticket Properties Form window (see page 67).

Tickets are generated by the system and sent to their designated owner (state=New; Status=Pending Action). Once they are opened, even if no action has been taken, the ticket state changes to Open. Depending on the ticket type, other types of action may be possible. When the ticket has been processed, the ticket state changes to Done, and you can archive the ticket.

As tickets can be hierarchal, that is actions taken on a ticket located higher in a ticket tree, can impact on a ticket lower in the tree. For example, a campaign ticket-tree consists of the Owner ticket (root-ticket) and the associated Approver tickets. The number of Approver tickets associated with a specific campaign is listed in the Children column (when visible). Until the Campaign-owner starts the campaign, the Approver tickets are listed in the campaign-owner's Ticket Queue as state=Hidden, and the Approver tickets do not appear in the respective approvers' Ticket Queues. Once the campaign has begun, the state of the Approver tickets listed in the campaign-owner's Ticket Queue changes to New. And the Approver tickets are now visible in their respective approvers' Ticket Queues. The approvers can now begin to examine the links provided in the Approver tickets.

Another facet of a ticket's life cycle is that some tickets, under certain conditions, can be transferred to another user. For example, a senior administrator can generate a campaign (the campaign-owner) and then transfer campaign ticket ownership to another system administrator. Approval Process tickets can also be transferred by their owners. The CA RCM Portal uses the terms delegate/escalate to denote such a transfer:

Delegate

The act of appointing a more-junior manager to be the ticket owner.

Escalate

The act of appointing a more-senior manager to be the ticket manager.

Note: The term “reassign” is used in relation to links, to mark the transfer of the responsibility for reviewing a link(s) from one Approver to another Approver.

More information:

Delegating a Campaign (see page 83)
Reassigning a Link (see page 100)

Ticket Types

A ticket's Ticket Type appears under the Type column in the user's Ticket Queue and also as the ticket title in the Ticket Properties Form.

The ticket type presents the ticket's purpose. Each ticket type has its own unique life cycle. Each ticket's state and status attributes denote where it is currently situated within the ticket's life cycle. Tickets can be part of a larger process, and therefore tickets in the same ticket type category, may actually present different functionality. The tickets are described in this manual as part of procedures, and therefore we have given them names according to their purpose within the procedure.

The following table presents the list of tickets described in this guide:

Name	Ticket Type(s)	Description
Campaign-owner ticket	Campaign	The campaign-root-ticket. The ticket generated and sent to the campaign-owner when a campaign is created. This ticket tree comprises the campaign ticket and all the campaign's Approver tickets. For more information see Running Campaign-owner Tickets (see page 77).
Approver ticket	Campaign Manager Approver	A ticket sent to a user, role or resource manager (depending on the campaign type). It contains the list of entity links that the entity's manager (Approver) has to approve. Each individual link can be approved, rejected or reassigned by the ticket owner to another approver. For more information see Campaign Approver Tickets (see page 95).
Info-ticket	Link [Entity1]-[Entity2] Delete Link [Entity1]-[Entity2]	Gives notice and supplies relevant information about specific situations in the ticket life cycle (for example. the termination of an approval process). For more information see Info-tickets (see page 72).
Approval Process Root ticket	Approval Root	A ticket generated after a campaign is stopped or completed. This ticket tree includes the Approver tickets associated with the campaign's rejected links that are being sent for review to the managers of the linked entities. For more information see Approval Process Tickets (see page 105).
Rejected-Link Parent ticket	Delete Link [Entity1]-[Entity2]	A ticket generated after a campaign is stopped or completed. This ticket is the specific rejected link's manager ticket. For each pair of Approver tickets sent to the link's entity managers, there is a parent ticket, thus creating a sub-tree for each rejected link. For more information see Approval Process Tickets (see

Name	Ticket Type(s)	Description
		page 105).
Approval Process Approver ticket	Delete Link [Entity1]-[Entity2]	A ticket generated after a campaign is stopped or completed. The rejected links are sent for re-evaluation to the managers of the linked entities. For example, a link between a role and resource will generate tickets to both the role manager and the resource manager. The Approver Ticket can be escalated/delegated to another approver by the ticket owner. For more information see Approval Process Tickets (see page 105).
Consult ticket	Delete Link [Entity1]-[Entity2]	A ticket generated when an Approver wishes to consult with another user, regarding the specific rejected link. For more information see Approval Process Tickets (see page 105).
Self-Service Approval Process Root ticket	Approval Root	The Self-Service request root ticket. A ticket generated when a self-service process requires approval from entity managers. For more information see Running Self-Service Tasks (see page 135).
Self-Service Request Parent ticket	Link [Entity1]-[Entity2] Delete Link [Entity1]-[Entity2] Update Role	This ticket is the specific Self-Service request manager ticket. For each set of Approver tickets generated for a Self-Service request, and sent to the link's entity managers, there is a parent ticket, thus creating a sub-tree for each rejected link.. For more information see Running Self-Service Tasks (see page 135) and Role Definition Tickets (see page 175).
Self-Service Approver Ticket	Link [Entity1]-[Entity2] Delete Link [Entity1]-[Entity2] Update Role	The Approver-tickets generated when a self-serviced process requires approval from entity managers. For more information see Running Self-Service Tasks (see page 135).
Self-Service Consult ticket	Link [Entity1]-[Entity2] Delete Link [Entity1]-[Entity2] Update Role	The ticket generated when a self-serviced process Approver wishes to consult another user regarding the specific request. For more information see Running Self-Service Tasks (see page 135).
Task	Task	A ticket generated when a specific task needs to be performed, usually as part of a larger procedure. For example, defining a new role's manager (accountable). For more information see Role Definition Tickets (see page 175).
Notification	Notification	A task ticket that is generated for the purpose of passing information.
Import/Export ticket	Import/Export	A ticket generated when an import or export event runs. For more information see Running a Connector

Name	Ticket Type(s)	Description
		(see page 248).
Error ticket	Error	Ticket generated when system error occur. For more information see Troubleshooting (see page 293).

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 Tables

The Ticket Queue enables you to display and interact with tickets, that are displayed in table format. You can view your own tickets and tickets that were generated by you, even though they have a different owner. The columns are customizable. The Ticket Queue menu provides a set of display filters. The available filters are:

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.

After selecting a display mode from the menu, you can interact with the tickets. You can:

- Expand a closed ticket-tree.
- Collapse an open ticket-tree.
- Click the owner's hyperlink to view the owner's data card.
- Sort the table based on one of the table's columns.
- Click the ticket title and open the Ticket Properties Form in a separate browser window. Here you can perform various operations, depending on the ticket type.

More information:

Sorting a Data Table by Column (see page 21)
Main Screen Layout (see page 63)
Main Screen Operations (see page 64)

Main Screen Layout

The Ticket Queue screen contains the following main features:

Menu Bar

Provides the Ticket Queue functionality.

Ticket table

Presents the various tickets.

The menu bar provides three functions:

- Search
- Customize
- Refresh

Users that were linked to the CA RCM Admin Role, have an additional option:

- User View/Admin View

The tickets are displayed in table format. The table is fully customizable and you can use the Customize function to select the columns (fields) that will appear in the tables and their order.

The default structure of the Ticket Queue table contains the following columns:

Field	Description
🚩	Marks an overdue ticket.
Ticket ID	Each ticket has a distinct ticket ID number.
Title	The ticket title.
State	The ticket's state.
Status	The ticket's status.
Children	The meaning of this number depends on the ticket type. For campaign-owner tickets, this provides the number of Approvers assigned to a specific campaign. For Approver tickets, this provides the number of entities listed in the ticket, whose links need to be reviewed.
Type	Provides the ticket type.
Received	Provides the date and time when the ticket was received.
Owner	The owner of the specific ticket. The functionality of the ticket changes according to who is viewing the ticket.

Field	Description
	Only the owner will have access to all the functions available for the specific ticket type.
Previous Owner	During campaigns or approval processes, tickets may be delegated/ escalated to other managers. If a ticket was sent to the owner from another user, that user's name (not the current owner) appears in this field.

As the Ticket Queue table can be customized, the columns that appear in the Ticket Queue table may be different than those presented here.

More information:

Administrator View / User View (see page 67)
Customizing a Data Table (see page 19)
The Tickets Pane (see page 50)

Main Screen Operations

The Ticket Queue menu bar provides five functions:

- Search
- Customize
- User View/Admin View
- Refresh
- Clear Filter (appears only when a Search filter has been activated)

This section covers the following topics:

- Search/Clear Filter
- Refresh

More information:

Customizing a Data Table (see page 19)
Administrator View / User View (see page 67)

Searching the Ticket Queue Table

Besides the basic filtering done by the Ticket Queue 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 Ticket Queue table.
Filter functions	The following filtering functions are available: ■ 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: ■ 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 Ticket Queue.

To search the Ticket Queue's table

1. Click Search on the Ticket Queue's 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 Ticket Queue's menu bar.
5. Click Clear Filter to return to the original filtered (by Ticket Queue menu options) ticket table.

Refresh

The Refresh button lets you update the contents of the current ticket table. It is especially useful following the performance of actions that change the ticket's state and/or status.

Click Refresh to update the ticket list displayed on screen.

Administrator View / User View

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

User View

The standard Ticket Queue 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 285)
CA RCM Properties (see page 305)

The Ticket Properties Form

When you click on a ticket listed in the ticket queue the Ticket Properties Form for that ticket opens in a separate browser window. The content of this screen depends on the type of ticket you are viewing.

The screen presents you with both data and functionality.

The top part of the screen is always the same and contains the ticket information:

Field	Description
<Ticket Title>	The type of ticket you are viewing appears in the screen's first line.
Ticket ID	Each ticket has a distinct ticket ID number.
Owner	The owner of the specific ticket. The functionality of the ticket changes according to who is viewing the ticket. Only the owner will have access to all the functions available for the specific ticket type.
Previous	During campaigns or approval processes, tickets may be

Field	Description
Owner	delegated/escalated to other managers. If a ticket was sent to the owner from another user, that user's name (not the current owner) appears in this field.
Status	Provides the ticket status.
Due Date	Each ticket has a due date, by which the action(s) ascribed to the ticket have to be performed.
Priority	Shows the current priority level. The available options are: ■ Low ■ Normal ■ Rush ■ Critical
Severity	Shows the current severity level. The available options are: ■ Minimal ■ Medium ■ Serious ■ Urgent ■ Critical
State	Shows the current ticket's state. The possibilities are: ■ New ■ Open ■ Hidden ■ Done ■ Archived ■ Canceled
Modified Date	Shows the date and time when the content of the ticket was last modified.
Date Created	Shows the date and time when the ticket was first created.
Title	The ticket's title.
Description	A description of the ticket.

More information:

Ticket Status (see page 61)

General Ticket Functions

Ticket functionality depends on the ticket type and on the user who is viewing the ticket. Every Ticket Properties Form has at least two active functions:

Save

Click to save any changes made to the ticket.

Close

Click to close the Ticket Properties Form browser window.

More information:

Running Campaign-owner Tickets (see page 77)
Campaign Approver Tickets (see page 95)
Running Self-Service Tasks (see page 135)

Advanced Ticket Functions

Advanced ticket functionality depends on the ticket type and is available only to the ticket owner. Click Advanced at the bottom of the Ticket Properties Form to access the advanced ticket functions.

Most non-info type tickets have the following functionality:

Add Comments

Click to add a comment to the ticket.

Add Attachments

Click to add an attachment to the ticket.

View Transaction Log

Click to view the ticket's transaction log.

Additional functions such as the option to view the ticket initiators, view violations or view the relevant user depend on the ticket type.

More information:

Running Campaign-owner Tickets (see page 77)
Campaign Approver Tickets (see page 95)
Approval Process Tickets (see page 105)
Info-tickets (see page 72)

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 ✗. Click ✗ 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 ✕. Click ✕ 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.

Info-tickets

Info-tickets provide users with notification of changes made to the system's configuration files. For example, when a role definition is updated, the role's manager is informed of the changes.

The info-ticket type is the same type as the ticket that was its origin. For example, an info-ticket sent following an approval by both a role manager and a user manager of a request to delete the link between the user and role will be of the type Delete Link User-Role.

Receiving an Info-Ticket

The following lists who receives an info-ticket and under what conditions:

Approval Process Owner

When an approval process has been completed.

Approver

When an approval process has been completed. As each approval process is submitted to two approvers, two such tickets are generated.

User

The user whose provisioning has been altered by the approval process is notified.

Role/Resource manager

The manager of the role/resource that has been updated is informed of the change(s).

As the ticket that was the origin of the modification of the universe's configuration can be of various types, the list of users can be longer or shorter, depending on whether one user has more than one role (a user is both the Approval Process owner and the user affected by the change), or if the ticket was delegated/escalated during the process.

General Info-Ticket Functionality

Info-tickets provide you with the following General functionality:

Close

Closes the ticket.

Save

Saves the changes made to the ticket.

Delegate

When you want to share the info-ticket's information, you can transfer the ticket to another manager.

Escalate

When you want to share the info-ticket's information, you can transfer the ticket to another manager.

Acknowledge

Click after reading the information provided by the info-ticket. The info-ticket is archived.

More information:

Delegate (see page 110)
Escalate (see page 108)

Delegating an Info-Ticket

This function lets you transfer the info-ticket to another manager, thus sharing important information. 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(s) is listed in the Previous Owner field.

A comment is generated stating that the ticket has been Delegated 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 (Ticket Queue, 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.

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

The Find 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 delegated 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.delegate.filter
```

To delegate a ticket

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

   The Find 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 Ticket Queue.

More information:

Add Comment (see page 70)
Filtering a Data Table (see page 20)
CA RCM Properties (see page 305)

Escalating an Info-Ticket

This function lets you transfer the info-ticket to a more senior manager, thus sharing important information. 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 (Ticket Queue, 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.

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

The Find 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 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 Ticket Queue.

More information:

Add Comment (see page 70)
Filtering a Data Table (see page 20)
CA RCM Properties (see page 305)

Advanced Info-Ticket Functionality

Info-tickets have standard advanced functionality, including:

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.

More information:

Add Comment (see page 70)
Add Attachment (see page 71)
View Transaction Log (see page 71)
View Parent (see page 113)
View Initiators (see page 113)

Chapter 7: Running Campaign-owner Tickets

Campaigns utilize CA RCM auditing tools to run a certification and attestation process. A campaign generates tickets for the designated approvers in the enterprise so that they can certify that the granted privileges comply with the business and regulatory needs, and are not over-allocated. Campaigns are used not only in the cleansing phase, but for periodic certification as required by law and various regulatory bodies.

Two types of tickets are generated for a campaign:

- Campaign-owner tickets
- Campaign Approver tickets

When a campaign is first created a campaign ticket is generated. This is the campaign-owner ticket. This ticket appears in the campaign-owner's Ticket Queue.

The campaign-owner ticket is structured as a tree where the top level (that is. the root-ticket) is the owner's ticket and the branches/leaves are the approvers' tickets. The Children column (when visible) in the campaign's root-ticket row, provides the number of Approvers assigned to a specific campaign. A campaign-owner can also be an approver, but it is not required. If there are entities that do not have assigned managers, their links will be sent to the campaign administrator for approval.

As the campaign proceeds and links are approved or rejected, reminders are sent and other tasks are performed, changing the content of the tickets and/or their State and Status. A campaign-owner can see all the tickets generated by the campaign, and can therefore follow the campaign by navigating the campaign's ticket tree.

Note: A campaign has to be manually started by the campaign-owner.

When you create a campaign and the campaign ticket is first created, its state is listed as New. After you open the ticket for the first time, its state is changed to Open. There are various actions a campaign-owner can take prior to starting a campaign (for example, escalate a campaign). The Approver tickets are listed as Hidden until you start the campaign. Once you start the campaign, the approvers can see the campaign tickets in their own ticket queue. A campaign can be manually stopped by the campaign-owner and later restarted if necessary. The campaign-owner can choose to archive a campaign ticket when he/she is done with it.

The status column provides additional information. When you first create a campaign, the status is Pending Action. After you manually start the campaign, the status changes to In Progress.

As the campaign-owner, you can open any ticket that appears in your campaign tree. You can therefore open Approver tickets and reassign the processes/links/entities listed within.

When you click on the campaign-ticket title, the top level of the campaign tree, the Ticket Properties Form opens in a separate browser window.

Campaign-Ticket data and general functions: Provides the ticket and campaign information. This section also provides several high-level functions, such as Close, Save.

Campaign Management provides the campaign management functionality.

Advanced provides additional functionality such as the ability to add comments or attachments; view the transaction log or view the campaign children.

This section contains the following topics:

Campaign-Ticket Data

In the Ticket Queue, select a campaign ticket. The campaign's Ticket Properties Form opens in a separate browser window.

The window presents the Campaign-Ticket Data in four sections:

Ticket data

In this section you can find the basic ticket data.

Functions

Provides the general campaign-ticket functionality.

General

Provides general data concerning the campaign.

Advanced

Lists the attachment and comments.

More information:

Ticket Data (Campaign) (see page 80)
General Data (Campaign) (see page 81)
Advanced (Campaign) (see page 82)

Ticket Data (Campaign)

The Ticket Data section consists of the fields located at the top of the campaign's Ticket Properties Form.

The Ticket Data section of the Campaign-Ticket Properties Form contains the following fields:

Ticket ID

The Ticket's unique number.

Owner

The Campaign-owner, the user who generated the campaign.

Previous Owner

During campaigns or approval processes, tickets may be delegated/ escalated to other managers. If a ticket was sent to the owner from another user, that user's name (not the current owner) appears in this field.

Status

Shows the current campaign-ticket status.

Due Date

The date by which the campaign-ticket must be completed.

Priority

Shows the current priority level.

Severity

Shows the current severity level.

State

Shows the current ticket's state.

Modified Date

The last time the campaign-ticket was modified.

Date Created

The date on which the campaign ticket was first generated.

Title

The campaign-ticket's title.

Description

The campaign-ticket's description.

General Data (Campaign)

The General section is in the body of the campaign's Ticket Properties Form.

The General section of the Campaign-Ticket Properties Form contains the following fields:

Universe

The name of the universe on which the campaign is being run.

Campaign Type

There are three possibilities:

User

A campaign in which the approvers certify the entitlements of the user under their management. The certification is in regard to the user's roles and resources. Improper entitlements can be rejected.

Role

A campaign in which the approvers certify the connection of the roles under their management. The certification is in regard to the role's linked users and resources. The certification also examines role-to-role hierarchal links. Improper entitlements can be rejected.

Resource

A campaign in which the approvers certify the connection of the resources under their management. The certification is in regard to the resource's linked users and roles. Improper entitlements can be rejected.

Auto Generate Permissions

True or False. When true, the campaign overrides the system permissions and automatically provisions the campaign permissions.

Audit Card

The name of the Audit Card.

Entity Filter

The entity filter.

More information:

Adding Campaigns (see page 222)

Advanced (Campaign)

The Advanced section appears below the campaign ticket's General section and above the Campaign Management section. It presents the list of attached files and/or links and any available comments concerning the campaign.

The Advanced section of the Campaign-Ticket Properties Form shows the attached file/URL and a comments table. Next to the attachment, you can see an ✕. Click ✕ to delete the attachment.

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 ✕. Click ✕ to delete the comment.

General Campaign-Ticket Functions

The Campaign section of the Ticket Properties Form contains all the campaign-ticket and campaign data.

This section also provides the following functions:

Close

Closes the Ticket Properties Form browser window.

Save

Saves any changes made to the campaign ticket.

Delegate

Allows you to delegate the campaign to a more junior manager. Once this is done, the campaign ticket will be relocated to your Ticket Queue archive.

Escalate

Allows you to transfer the campaign to a more senior manager. Once this is done, the campaign ticket will be relocated to your Ticket Queue archive.

Delegating a Campaign

This function allows you to delegate the campaign to another administrator. Once you have selected the new campaign administrator, the campaign's ticket is archived and will no longer appear in your list of active tickets.

When a campaign is delegated, a new root-ticket is generated with the new owner listed in the Owner field and the administrator who delegated the campaign 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.

The new root appears as the top-level in the new "owner's" campaign ticket, and as the second level in the previous owner's archived campaign ticket.

To delegate a campaign, 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:

```
tms.delegate.filter
```

To delegate an campaign

1. Click Delegate in the Campaign-Ticket's 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 campaign is archived and its status is set to Delegated. The campaign ticket appears in the target user's Ticket Queue.

More information:

Filtering a Data Table (see page 20)
CA RCM Properties (see page 305)

Escalating a Campaign

This function provides you with the option to transfer the campaign management to a more senior manager. Once you have selected the new campaign administrator, the campaign's ticket is archived and will no longer appear in your list of active tickets.

When a campaign is escalated, a new root-ticket is generated with the new owner listed in the Owner field and the administrator who escalated the campaign is listed in the Previous Owner field.

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

The new root appears as the top-level in the new "owner's" campaign ticket, and as the second level in the previous owner's archived campaign ticket.

To escalate a campaign, 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 an approval

1. Click Escalate in the Campaign-Ticket's 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 campaign is archived and its status is set to Escalated. The campaign ticket appears in the target user's Ticket Queue.

More information:

Filtering a Data Table (see page 20)
CA RCM Properties (see page 305)

Campaign Management Functions

The campaign management section of the Ticket Properties Form screen provides the following functions:

Start Campaign

The campaign won't start and approver tickets will remain hidden until the campaign is activated. When you start a campaign, the state changes to New. An email notification is sent to all the campaign's Approvers, notifying them that a campaign has begun and that they have links to approve.

Stop Campaign

This allows you, as the campaign-owner, to arbitrarily stop a campaign at any time.

Restart Campaign

This function is active only after a campaign has been stopped.

Archive

Provides you with the option of moving the campaign from the main ticket table to the archive.

Generate Campaign Results Configuration

Aborts the approval process and outputs the results of the campaign to configuration files.

Start Approval Processes

As the campaign progresses not all the links are approved. The rejected links have to be sent through a secondary approval process.

View Campaign Progress

Opens a separate browser window where you can view the campaign progress for each individual approver.

Send Reminder

Lets you send email reminders to approvers whose performance is not acceptable under the campaign's deadline.

More information:

Approval Process Tickets (see page 105)

Running the Campaign

This section examines the management options available on the campaign ticket.

Start Campaign

Once you have added a campaign to the system and the campaign ticket has been generated, it resides in your Ticket Queue. Until you, as the campaign-owner, start the campaign, none of the approvers assigned to this campaign will be able to view their Approver tickets, and the approval process will not begin.

Starting the campaign creates the following changes:

Field	Before	Start Campaign
State (Campaign-owner ticket)	New/Open	Open
Status (Campaign-owner ticket)	Pending Action	In Progress
Approver tickets	Hidden from approvers	Visible to approvers

Click Start Campaign in the campaign's Ticket Properties Form, to get the campaign going.

All the campaign's Approvers will receive notice of the new campaign in the email designated by the CA RCM master configuration.

Stop Campaign

You, as the campaign-owner, can wait for all the approvers to complete their review or you can manually stop the campaign. A campaign that was manually stopped can later be restarted.

When a campaign has been stopped, it returns to its pre-start conditions: state=Open, status=Pending action, and the approver tickets are once again hidden from their owners.

Click Stop Campaign in the campaign's Ticket Properties Form to manually stop a campaign.

More information:

Restart Campaign (see page 88)

Restart Campaign

The ability to restart a campaign is enabled only when you manually stop a campaign.

When you restart a campaign, the approver tickets are once again accessible to the Approvers. You will see them listed as state=New in your Ticket Queue, but their status will reflect their status prior to the campaign's manual cessation. For example, if an Approver managed to complete his assigned reviewing tasks while the campaign was running, this Approver's ticket status will be Completed. After you restart the campaign, this Approver ticket's status will show that the process has been already completed.

Click Restart Campaign in the campaign's Ticket Properties Form, to restart a campaign that had been manually stopped. An email notification is generated and sent to all the campaign's Approvers.

Start Approval Processes

The approval process is the procedure whereby links, which were rejected during a campaign, can be re-examined and a final decision can be reached as to whether to confirm the rejection or to approve the link.

The purpose of a campaign is to audit and certify entity links. Once a campaign is over (either because all the approvers have audited all the entity links, in their Campaign-Approver tickets, or because the campaign was manually stopped) it is necessary to review all the rejected links once more, as the final step in the certification process.

To start the approval process

1. Click Start Approval Processes in the campaign's owner-ticket.

   A confirmation prompt appears.

2. Click Yes to confirm.

   The Executing bar appears.

More information:

Approval Process Tickets (see page 105)

Archive

This feature allows you to completely shut down a campaign by transferring it to your archived tickets. While a campaign that has been manually stopped can be restarted, an archived campaign cannot be rerun. By archiving a campaign while it is running, you also close down the ability to run approval processes on any links that have already been processed and rejected during the time the campaign was active.

Archiving a campaign after it has been completed but before the Approval Processes have been run, will prevent any possibility of running an approval process based on this campaign's rejected links.

To archive a campaign

1. Click Archive in the campaign's Ticket Properties Form, to manually archive a campaign.

   A confirmation prompt appears.

2. Click Yes.

   The campaign is archived and completely shut down.

Generate Campaign Results Configurations

Most certification campaigns involve two phases:

- **Review—**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 the role can access.
- **Approval—**If a link is rejected during the review phase, 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 trigger approval tasks, because they change the base configuration.

You can abort the approval process for your campaign, and have CA RCM save the results of the review phase as configuration files. You can then initiate campaigns or other processes based on these output configurations. For example, you can submit the rejected links to another set of reviewers.

Two configuration files are generated. One contains all the links that were rejected during the review phase, and one contains all the links that were approved. CA RCM labels the two files using the following naming convention:

Rejections_*campname*

Approvals_*campname*

Note: *campname* is the name of the original campaign.

The Create Campaign Results Configurations option appears in the campaign ticket. It is enabled when the campaign state is Stopped.

Note: If you stop the campaign after changes are approved, those changes are implemented in the base configuration even if you click the Create Campaign Results Configurations option.

The following system property controls this option:

campaign.settings.allowCreateCampaignResultsConfigurations

Specifies whether the Create Campaign Results Configurations option is available on the portal.

True

Displays the Create Campaign Results Configurations option in the campaign ticket.

False

Hides the Create Campaign Results Configurations option.

View Campaign Progress

The progress of the campaign is measured by the number of links that need to be audited by the various campaign-approvers, and have already been approved or rejected. The View Campaign Progress function opens a separate browser window where you can see a listing of all the campaign's approvers and view the progress they have made graphically, numerically and in percentages.

The header of this window contains the following information:

[Title] Progress

Provides the name of the campaign-ticket.

Universe

Provides the name of the universe on which the campaign is being run.

Configuration

Provides the name of the configuration on which the campaign is being run.

The progress table contains the following columns:

Approver

The Approver ID.

Name

The Approver name.

Progress

A graphical presentation of the amount of progress each Approver has made.

Completed

Shows numerically [# of links have been audited]/[total # of links to be audited], for example 0/40 means that none of the 40 links to be audited have been approved, rejected or reassigned. This table also provides the value as a percentage. For example: 1/3 (33%).

When available, you can control the number of records listed per page using the Records per page function at the bottom of the table.

Configure Escalation E-mails

The campaign-owner can send emails to remind the approvers that they have to meet the campaign goals in a timely fashion. you can set completion criteria to automatically trigger emails to approvers based on their completion status.

When an email is sent to an approver, a comment appears in your Campaign-owner ticket in the Comments table.

To configure escalation emails

1. Click Escalation E-mailsin the Ticket Properties Form.
2. Configure the completion criteria, email target, and template for escalation emails.
3. Click Save

   Settings are saved.
4. Click Send Now to send emails immediately.

Campaign-Ticket Advanced Functions

The Advanced button located at the bottom of the Ticket Properties Form provides you with the following functions:

- Add Comment
- Add Attachment
- View Transaction Log
- Open Children

Click Advanced to access the advanced campaign ticket functions.

More information:

Add Comment (see page 70)
Add Attachment (see page 71)
View Transaction Log (see page 71)
View Children (see page 93)

View Children

Campaign tickets are set up as hierarchal trees. The Open Children option allows you to see information concerning all the leaves that are located below the Campaign Ticket. This includes all campaign's Approver-Tickets. You can control the number of records per page listed in the table by using the Records per page option.

The following fields appear in the Children table:

Action

The action you can take concerning this ticket. For example: Select opens the selected ticket in a separate browser window.

Owner

The ticket owner.

Type

The ticket type.

Status

The ticket status.

Title

The ticket title.

Comments

The last comment added to this ticket.

To view a ticket's children tickets

1. Click Advanced at the bottom of the Ticket Properties Form screen.
2. Click Open Children.

   A table opens at the bottom of the Ticket Properties Form screen.
3. Click Close Children to close the ticket-children table.

Campaign Approver Tickets

When you create a new campaign, you can see all the Approver tickets associated with your campaign as well as the main campaign ticket and your own Approver tickets (where relevant). The Approver tickets are listed in your ticket queue as branches of the campaign-ticket tree.

Which entity managers are assigned to a campaign as approvers depends on the nature of the campaign.

- For a user certification campaign, user managers will be assigned as approvers.
- For a role certification campaign, role managers will be assigned as approvers.
- For a resource certification campaign, resource managers will be assigned as approvers.

Each approver is in charge of reviewing the links between the entity they are managing and the other entity types. For example, in a user certification campaign, user managers will be charged with reviewing their team's links to roles and resources.

You can open any of the Approver tickets, view the contents and reassign any of the listed entity links.

You cannot add comments, attachments, view the initiators or view the transaction log from within a Ticket Properties Form that you do not own (see Owner field in the upper part of the screen).

More information:

Campaign Approver Tickets (see page 95)
Auditing Links (see page 97)

Chapter 8: Campaign Approver Tickets

This chapter is intended for users who receive Campaign Manager Approver (CMA) tickets.

When a new campaign is generated, CA RCM generates Campaign Manager Approver (CMA/Approver tickets) tickets. Entity managers are assigned to a campaign as approvers based on the campaign type. For example, for a user certification campaign, user managers 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, that is 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 a campaign targeting your entity.

As an approver, your job is to review the links between the entity you are managing and the corresponding entity types. The information appears in the CMA ticket as trees of links, where the campaign's entity type and the linked entities are presented in a nested arrangement. This means that if you are a role manager, and you received a CMA ticket as part of a Role campaign, you will see lists of roles that can be expanded to show the nested entity links with Users, Resources, Child Roles and Parent Roles.

When viewing the CMA in the Ticket Queue, you can see how many campaign-type entities you have to review by checking the Children column. A role manager with 10 listed in the Children column has to audit ten roles and their links to their users, resources, Child roles and Parent roles within the campaign's configuration files.

Note: The **default maximum number of entity trees per page is 10.**

The certification is complete when you have reviewed all the links listed in the ticket and either approved, rejected or reassigned (when relevant) them.

The campaign-owner can view all the CMAs as branches located under the campaign's owner ticket. Other users can only view their own CMAs.

Note: The campaign-owner can stop a campaign whenever he chooses to do so. If he does, the Campaign Manager Approver tickets will be hidden from the Approvers.

Approver (CMA) tickets contain two types of operations:

- Link related actions
- Ticket related actions

Ticket related actions that are shared by all ticket. Ticket related actions unique to specific types of tickets are described in the relevant sections.

This section contains the following topics:

CMA Ticket Properties Form

As an approver, your goal is to examine the links listed within your CMA ticket and approve, reject or reassign them by the campaign's due date.

As you review progresses (after every time you save your selections) you can see your progress on the Approver Progress bar. Your progress is also listed as:

[number of links approved]/[total # of links to approve]

so that if you have a total of six links to approve, and you have already approved two links, you will see 2/6 in digits and the percentage, 33%, listed next to it.

More information:

Tickets and the Ticket Queue (see page 55)
The Ticket Properties Form (see page 67)
Auditing Links (see page 97)
General CMA Ticket Functions (see page 103)
Advanced CMA Ticket Functions (see page 104)

Auditing Links

The CA RCM Portal generates Campaign Manager Approver tickets (Approver tickets/CMA tickets) as part of a campaign. These tickets contain links that have to be examined. The Approver is responsible for approving, rejecting or reassigning links between entities.

This section describes actions available for Approver tickets:

- Presenting the Entity Links Table
- Approving a link
- Rejecting a link
- Reassigning a link
- Adding comments to a specific link

Presenting the Entity Links Table

Campaign-Manager-Approver tickets (CMA/Approver tickets) present all the links for each entity listed in the ticket, based on the campaign definitions. Every Approver ticket presents the links in an entity-link table. When you first open the CMA's Ticket Properties Form, you will find that the hierarchal entities tree is collapsed. The visible entity is the target of the campaign. For example, in a user campaign you will see a table of users.

When you expand the tree for each entity listed in the table, you will see entity tables for the linked entities. The following table describes the entity tables found in each Approver-Ticket type:

User Campaign CMA

Main entity table: Users

Link-tables: Roles and Resources

Role Campaign CMA

Main entity table: Roles

Link-tables: Users, Resources, Child Roles and Parent Roles

Resource Campaign CMA

Main entity table: Resources

Link-tables: Users and Roles

Note: Only the ticket owner can approve or reject a link. The campaign-owner can reassign a specific link within a Campaign-Approver ticket to another approver.

Three columns in entity table contain check boxes with icons in the column header. Sometimes a fourth icon appears in a row.

The icons associated with the entity tables are as follows:

Icon	Description
⊞	Expands the nested links tree, showing the entities linked to the original entity. For example, in a user certification-campaign Approver ticket, each user is linked to roles and resources. Clicking on the ⊞ will reveal the linked Roles and Resources in separate tables.
!	Additional information.
✓	The Approve checkbox column. Click this checkbox to approve a link.
✗	The Reject checkbox column. Click this checkbox to reject a link.
➡	The Reassign checkbox column. Click this checkbox to reassign a link.
⊟	Collapses the link tree.

Click ⊞ to expand the entity tree and see all the entity tables for the entities linked to this entity.

Click ⊟ to collapse the entity tree.

The main Entity Table columns are predetermined. They depend on the campaign type. However several columns appear in all types of Main Entity tables:

Progress

Shows the progress made in examining the current entity.

Violations

Records violations based on the Audit Card data.

Comment

Allows you to assign a comment to a specific link.

The Link-Entity table columns are also predetermined. They depend on the entity being presented in the specific table. However several columns appear in all Link-Entity tables:

Violations

Records violations based on the Audit Card data.

History

Presents the history of the link between the main entity and the entity listed in the selected row.

Comment

Allows you to assign a comment to a specific link.

Approving a Link

Once a link is approved and the ticket is saved, the audit process for this entity link is over.

Note: You can approve all the links listed in a specific link-table at once by clicking the column label ✓ for that link-table.

To approve a user link

1. In the Ticket Properties Form click ⊞ next to the user you wish to audit.

   The associated Roles and Resources tables appear.

2. Click the check box in the ✓ column, next to the user’s role(s) and/or resource(s) that you want to approve.
3. Click Save.

   The selected links are approved and the relative progress made is reported on the Approver Progress bar.

Note: Replace “user” in the above procedure with either “resource” or “role” for instructions on how to approve Role links or Resource links.

Rejecting a Link

When a link is rejected during a campaign, the rejection does not become final until it is reviewed and confirmed during the Approval Process by the link's entity managers. For example, when a link between a user and a role that has been rejected, both the user's manager and the role's manager have to confirm that this link should be rejected. Only then is the decision final. Users whose links are rejected will be informed of the rejection.

Note: You can reject all the links listed in a specific link-table at once by clicking the column label ✗ for that link-table.

To reject a user link

1. In the Ticket Properties Form click ⊞ next to the user you want to audit.

   The associated Roles and Resources tables appear.

2. Click the check box in the ✗ column next to the user's role(s) and/or resource(s) that you want to reject.
3. Click Save.
4. The selected links have been rejected and the relative progress made is reported on the Approver Progress bar. The system default accepts the rejection as final only after the Approval Process.

Note: Replace "user" in the above procedure with either "resource" or "role" for instructions on how to reject Role links or Resource links.

Reassigning a Link

The CA RCM Portal allows managers to choose to reassign a link listed in their CMA ticket for review, to another Approver. Therefore, you, as an Approver ticket owner, can reassign any link listed in your Approver tickets. When the reassignment process is completed, a notice is sent automatically to both your email inbox and to the Approver who was reassigned the link.

Campaign-owners can also decide to reassign links listed in specific Approver tickets, so that they will now appear in the newly assigned entity manager's ticket. The Approver who was reassigned the link will see the relevant ticket in his/her ticket queue.

When you click the Save and Reassign button, any changes already made to the ticket are saved. Then the Find Reassign Users screens opens in a separate browser window.

The screen is divided into of two sections:

- Users Filter
- List of possible approvers

The list of users provided in this screen is governed by the following property:

```
tms.campaign.[entity]Certification.reassign.filter=GFilter= [specific filter]
```

Once you select the user to whom you intend to reassign the link, the →👤 appears next to the selected row in the entity table.

You can view the reassignment details in a ToolTip that appears when you move the pointer over the →👤 icon.

The target user can view the reassignment details as a ToolTip marked by ℹ, which is located in the **!** column.

Note: You can reassign all the links listed in a specific link-table at once by clicking the column label ➔ for that link-table.

Important! Do not click the column label ➔ unless you want to reassign all the links to one single user.

If the reassignment process generates a new ticket (i.e. the target user did not have an Approver ticket as part of the current campaign), it is called a Campaign Reassigned Approver ticket and the reassignment details will be posted above the Approver Progress bar in the target Approver's new ticket.

To reassign a user link

1. In the Ticket Properties Form click ⊞ next to the user you wish to audit.

   The associated Roles and Resources tables appear.

2. Select the check box in the ➡ (reassign) column, next to the user's role(s) and/or resource(s) you want to reassign.

   Note: If you select more than one role/resource, they will all be reassigned to the same Approver.

3. Click Save and Reassign. The Find Reassign Users screen opens in a separate browser window.
4. (Optional) Click Select to filter the table.
5. Select a user from the list. Click OK.

   The selected links have been reassigned and the relative progress made is reported on the Approver Progress bar. You see the icon ➡👤 next to the reassigned link in the entity table.

Note: Replace “user” in the above procedure with either “resource” or “role” for instructions on how to reassign Role links or Resource links.

More information:

Filtering a Data Table (see page 20)
CA RCM Properties (see page 305)

Adding Comments to Links

The Approver ticket’s Entity Link table provides you with the option to add comments next to specific links.

You can add comments next to the main entity (collapsed table), or next to a specific link in the expanded entity table.

To add a comment to a link

1. Go to the record where you want to add the comment. Click ✎ in the selected row (in the Comment column).

   A free style text box opens.

2. Enter the free style text of your choice.
3. Click the column label Comment, at the top of the Entity Table.

   The comment is added to the Entity Table.

More information:

Add Comment (see page 70)

General CMA Ticket Functions

The Campaign-Manager-Approver ticket provides the following functions:

Close

Closes the ticket.

Save

Saves the changes made to the ticket.

Save and Reassign

Provides the option to reassign a link and save the change.

Hide Selected

Hides the entities whose links have already been reviewed. When active the Show all button appears.

Show All

Reveals all the hidden links

More information:

Reassigning a Link (see page 100)
Hide Selected (see page 103)

Hide Selected

This feature hides the entities, that have already been examined. This function will only hide those entities whose entire list of links has been reviewed. As any manager can have many entities that need to be reviewed, this option makes it easier to see which entities have links that have not been reviewed.

It is important to realize that the function only hides main-entities that have been fully audited. Entities whose link-tables have only been partially audited will be visible.

IWhen the Hide Selected option is active, the function menu bar changes and replaces the Hide Selected button with a Show All button.

Advanced CMA Ticket Functions

The Campaign-Manager-Approver ticket provides the following advanced functions at the bottom of the CMA's Ticket Properties From:

More information:

Add Comment (see page 70)
Add Attachment (see page 71)
View Transaction Log (see page 71)
View Initiators (see page 104)

View Initiators

The View Initiators button opens the View Initiators list in a separate browser window. This list (in table format) provides the list of users that generated this Campaign-Manager-Approver ticket. Usually, you can find here the name of the campaign-owner. When a campaign has been delegated or escalated, you can view the list of users who received ownership of the campaign.

The information provided by the View Initiators table is based on the campaign's configuration files.

To view the campaign's initiator list

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

   The View Initiators table appears in a separate browser window.

Chapter 9: Approval Process Tickets

This chapter is designed for managers who can run post-campaign Approval Processes and for entity managers who may receive Approver tickets as part of the approval process.

Note: As the post-campaign Approval Process is always started by the current campaign-owner, the owner of the Approval Process tree's root ticket will be designated in this chapter as the "campaign-owner", even if the current owner of the ticket is actually someone who received the ticket during the Approval Process as a result of an escalation or delegation operation.

Following a campaign, your next task is to review all the rejections that were generated in the course of the campaign. As you know, the campaign itself is a straightforward review of the current links present within the campaign's selected universe and configuration from a specific entity's point of view. As such, during a campaign you can approve or reject a link, but the final decision regarding rejected links is postponed. The Approval Process sends every rejected link to the managers of the involved entities (both sides of the link), allowing them the final say as to whether to reject the link or not.

This means that during the approval process

- Tickets will be sent to both the user manager and the role manager of each rejected user-role link
- Tickets will be sent to both the user manager and resource manager for each rejected user-resource link.
- Tickets will be sent to both the role manager and the resource manager for each rejected role-resource link.
- Tickets will be sent to the role manager(s) for each rejected role-role (hierarchy) link.

Note: The rejection or approval of a link during this process is final and will not be sent for further review.

The approval process is started by the current campaign-owner. When an instruction to begin an Approval Process is given, the CA RCM generates a hierarchal Approver Process ticket tree. The ticket tree comprises three nodes:

Approval Root ticket

This ticket belongs to the campaign-owner. Each approval process has only one root ticket..

Rejected-Link Parent Ticket

This is a Delete Link [Entity1]-[Entity2] ticket. This ticket belongs to the campaign-owner. 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 rejected-links being processed.

Approver Tickets

This is a Delete Link [Entity1]-[Entity2] ticket. Two tickets of this kind are generated, one for each entity manager, per each rejected link. For example, when the rejected link is a user-role link, then one ticket will go to the user's manager and the second ticket will go to the role's manager

Entity managers are assigned as approvers to an Approval Process 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 representation under Accountable, that is 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.

The campaign-owner has overall control of the approval process. They can transfer responsibility of the process to another manager or cancel the process when necessary. This can be done for the complete ticket tree or for a single sub-tree.

As an approver you are tasked with making the decision whether to approve the rejection 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 track the ticket and 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:

General Approval Process Ticket Functions

The Ticket Properties Forms for the various Approval Process tickets share many of the same functions. The following table provides a summary of all the General functions available for the various Approval Process tickets.

Ticket Type	Functions
Approval Root (campaign-owner ticket)	Close, Save, Delegate, Escalate, Start Process, Cancel Process, Acknowledge, More Details/Less Details
Delete Link [Entity1]-[Entity2] (Rejected-Link Parent ticket)	Close, Save, Delegate, Escalate, Cancel Process, More Details/Less Details
Delete Link [Entity1]-[Entity2] (Approver ticket)	Close, Save, Delegate, Escalate, Consult, Approve, Reject, More Details/Less Details

Besides the Ticket Properties Form General functions, the following functions can be found in all of the tickets:

- Escalate
- Delegate
- More Details/Less Details

The functions that are unique to the various tickets will be described in the relevant sections.

- Approval Root (campaign-owner)
- Delete Link [Entity1]-[Entity2] (campaign-owner)
- Delete Link [Entity1]-[Entity2] (Approver ticket)

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 (Ticket Queue , 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 Ticket Queue (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 Ticket Queue.

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

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 Ticket Queue.

More information:

Add Comment (see page 70)
Filtering a Data Table (see page 20)
CA RCM Properties (see page 305)

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 (Ticket Queue, 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 Ticket Queue (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 Ticket Queue.

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

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:

```
tms.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 Ticket Queue.

More information:

Add Comment (see page 70)
Filtering a Data Table (see page 20)
CA RCM Properties (see page 305)

More Details/Less Details

The More Details>> and <<Less Details buttons, located below the general function buttons, toggle between showing additional data and hiding the same data.

The data fields and their content depend on the ticket type and it is in general self-explanatory.

To toggle between the two modes click the visible option More Details/Less Details.

Advanced Approval Process Ticket Functions

The Ticket Properties Forms for the various Approval Process tickets share many of the same functions.

- Add Comment
- Add Attachment
- View Transaction Log

The following Advanced functions are described in this section:

- View Initiators
- View Parent
- View Children
- View [Entity] [where entity is either user, role or resource]

The following table provides a summary of all the Advanced functions available for the various Approval Process tickets:

Ticket Type	Advanced Functions
Approval Root (campaign/Approval Process owner ticket)	■ Add Comment ■ Add Attachment ■ View Transaction Log ■ View Children ■ View Statistic
Delete Link [Entity1]-[Entity2] (Rejected-Link Parent ticket)	■ Add Comment ■ Add Attachment ■ View Transaction Log ■ View Parent ■ View Initiators ■ View Children ■ View Entity1 ■ View Entity2
Delete Link [Entity1]-[Entity2] (Approver ticket)	■ Add Comment ■ Add Attachment ■ View Transaction Log ■ View Parent

Ticket Type	Advanced Functions
	■ View Initiators ■ View Violations ■ View Entity1 ■ View Entity2 ■ View Consult Results (toggle)

More information:

Advanced Ticket Functions (see page 69)

View Initiators

The View Initiators button opens the View Initiators list in a separate browser window. This list (in table format) provides the sequence of users who that launched this post-campaign Approver Process ticket. For example, you can find here the name of the campaign-owner. When a ticket has been delegated or escalated, you can view the list of users who received ownership of the ticket.

The information provided by the View Initiators table is based on the campaign's configuration files.

To view the ticket's initiator list

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

   The View Initiators table appears in a separate browser window.
3. Click Close to close the View Initiators window.

View Parent

Post-campaign Approval Process tickets are set up as hierarchal trees. The View Parent option provides you with quick access to the current ticket's parent ticket. When you click View Parent in the Ticket Properties Form's Advanced functions section, the parent ticket opens in a separate browser window.

For the Approval Process ticket tree, this means that you can view the parent tickets for the Request Parent ticket and for each Approver ticket..

Click View Parent to open the current ticket's parent ticket in a separate browser window.

View Children

Post-campaign Approval Process tickets are set up as hierarchal trees. The View Children option allows you to see information concerning all the nodes/leaves that are located below the current ticket. For the Approval Process ticket tree, this means that you can view the children tickets for the Approval Process Root ticket and for the Rejected-Link Parent ticket.

You can control the number of records per page listed in the table by using the Records per page option.

The following fields appear in the View Children table:

Action

The action you can take concerning this ticket. For example: Select opens the selected ticket in a separate browser window.

Owner

The ticket owner.

Type

The ticket type.

Status

The ticket status.

Title

The ticket title.

Comments

The last comment added to this ticket.

To view a ticket's children tickets

1. Click Advanced at the bottom of the Ticket Properties Form screen.
2. Click View Children.

   A table opens at the bottom of the Ticket Properties Form screen. The View Children>> button becomes the <<Close Children button.
3. (Optional) Click Select in the Action column to navigate to the ticket listed in that row.

   The selected ticket opens in a separate browser window.
4. Click Close to close the selected ticket.
5. Click Close Children to close the ticket-children table.

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.

More information:

The Entity Card (see page 22)

Approval Process Root-Ticket

The Approval Root-ticket is the root-ticket that appears in the Ticket Queue belonging to the manager/administrator who started the Approval Process. When expanded, you can see a set of sub-trees, one for each rejected-link that has to be reviewed.

The number of sub-trees for any Approval Process Root ticket is listed in the Ticket Queue's Children column. Each sub-tree consists of a Rejected-Link Parent ticket and two Approver tickets, one for each of the entities that make up the rejected link that is being reviewed.

Note: Under some circumstances, only a single ticket is located below a Rejected-Link Parent ticket. The ticket is then a Notification ticket that informs you of the reason why the expected approver tickets are not present.

When you click the ticket title you open the Ticket Properties Form in a separate browser window.

In this section you will find information specific to the Approval Root-ticket type. It is important to remember that Approval Process tickets are based on specific campaigns.

The following fields give you the basic information concerning the current Approval Process:

<Ticket Title>

Approval Root

Title

[*Campaign Title*] Approval Root Request

Description

A description of the ticket. It includes the details of the request: Request submitted on Universe [Universe name] from [Campaign Title]

This section covers the following topics:

- The Approval Root ticket's General functions
- The Approval Root ticket's Advanced functions

More information:

Rejected-Link Parent Ticket (see page 119)
The Ticket Properties Form (see page 67)

Approval Root Ticket General Functions

The 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' Ticket Queues.

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.

This section provides instructions for the following functions:

- Cancel Process
- Acknowledge

More information:

Delegate (see page 110)
Escalate (see page 108)
Cancel Process (see page 117)
Acknowledge (see page 118)

Cancel Process

As the Approval Process owner, you have the authority to cancel an Approval Process when necessary. When you choose to cancel an Approval Process, click Cancel Process and a Confirmation pop-up window opens.

Click Yes to cancel the current Approval Process and the Executing bar appears. When done, the ticket (and it's tree) no longer exist.

Acknowledge

When you first open the Approval Root ticket, you will find that the Acknowledge button is disabled. It will only be enabled when all the Approver tickets belonging to the ticket tree will be reviewed and each request either rejected or approved.

Click Acknowledge to finish the Approval Process. The Executing bar appears. When the process is complete, the ticket is archived.

Approval Root Ticket Advanced Functions

The 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' Rejected-Link Parent ticket.

View Statistics

Provides the status of all the children tickets.

More information:

Add Comment (see page 70)
Add Attachment (see page 71)
View Transaction Log (see page 71)
View Children (see page 114)
View Statistics (see page 118)

View Statistics

The View Statistics button opens the View Statistics list in a separate browser window. This list (in table format) presents the statistics concerning how many of the child tickets (Reject-Link Parent ticket, in this case), have one of three state/status combinations. Any ticket that has already been processed will not be listed here.

To view the ticket's statistics information

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

   The View Statistics table appears in a separate browser window.
3. Click Close to close the View Statistics window.

Rejected-Link Parent Ticket

The Rejected-Link Parent ticket is a management ticket, generated by the CA RCM portal for every rejected link that has to be reviewed during an Approval Process procedure. While the Approval Root ticket controls the lifecycle of the whole tree, the Rejected-Link Parent ticket controls the lifecycle of the individual link under its purview.

In this section you will find information specific to the Rejected-Link Parent ticket. It is important to remember that Approval Process tickets are based on specific campaigns.

<Ticket Title>

Delete Link [*Entity1*] [*Entity2*]. For example: Delete Link User-Resource.

Title

Request to remove [*Entity1*] to [*Entity2*] association. [*Entity1*]: [*Entity1-name*], [*Entity2*]: [*Entity2-name*]. For example: Request to remove user to resource association. resource:'UGMPMRK,RACFPROD,RACF22 (Production RACF)' ,user:'Garr Jim (77371120)'.

Description

A description of the ticket. It includes the details of the request: Request was submitted on Universe [Universe name] from [Campaign Title]. For example: Request to remove user to resource association. resource:'UGMPMRK,RACFPROD,RACF22 (Production RACF)', user:'Garr Jim (77371120)' - Request was submitted on Universe Portal from User Review.

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 tree.

More information:

The Ticket Properties Form (see page 67)

Rejected-Link Parent Ticket General Functions

The Rejected-Link 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 110)
Escalate (see page 108)
Cancel Process (see page 117)

Rejected-Link Parent Ticket Advanced Functions

The Rejected-Link 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 Reject-Link Parent ticket, this means that you can view information concerning the link's Approver tickets.

View [Entity]

Opens the entity's card. Two buttons are provided, one for each member of the link under review.

The View Children function shows you the two Approver tickets associated with this parent ticket:

You can access the corresponding Approver tickets by clicking Select in the ticket's row.

More information:

Add Comment (see page 70)
Add Attachment (see page 71)
View Transaction Log (see page 71)
View Initiators (see page 113)
View Parent (see page 113)
View [Entity] (see page 115)
View Children (see page 114)

Approval Process Approver Tickets

When an Approval Process is set it motion, following a campaign, the Approver tickets are sent to all the relevant entity managers. As an Approver, your job is to either approve or reject the request to reject a link between two specific entities. The Approver ticket supplies you with all the data you need to make the decision and with the required functionality to assist you in the process.

The Ticket type's name is constructed from the ticket's action and the entities involved. Therefore, an Approver ticket for a request to remove a link between a user and a resource will be called a Remove Link User-Resource ticket.

Your main task is to either approve or reject the submitted request to sever a link between two entities. You can use any of the ticket's functions to find out more information or perform any related task.

This section covers the following topics:

- Approver tickets' General functions
- Approver tickets' Advanced functions

More information:

Reject (see page 125)
Approve (see page 125)

Approver Tickets General Functions

The Approval Root ticket provides the following General functionality:

Close

Close 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 request to delete the link between the two entities. Once approved, the link is severed.

Reject

Reject the request to delete the link between the two entities. This means that the link will not be severed.

More information:

Delegate (see page 110)
Escalate (see page 108)
Approve (see page 125)
Consult (see page 123)
Reject (see page 125)

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 Ticket Queue.

The consult ticket that is generated is sent to each consultant’s Ticket Queue.

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.

If you click View Parent, you will see the ticket from which the consultation request originated (all functions disabled).

When you have selected to either 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 Ticket Queue.

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

More information:

Filtering a Data Table (see page 20)

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.

More information:

Approval Process Info-Tickets (see page 127)

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.

More information:

Approval Process Info-Tickets (see page 127)

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 is disabled for Approval Process tickets.

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 70)
Add Attachment (see page 71)
View Transaction Log (see page 71)
View Initiators (see page 113)
View Parent (see page 113)
View [Entity] (see page 115)
Consult (see page 123)

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.

Approval Process Info-Tickets

When specific Approver ticket's owner completes an approval process, that is the designated Approvers approved or rejected a request to sever a link between two entities, all the users connected to the process are informed of the decision. The CA RCM Portal sends a ticket to inform the concerned parties that a change has taken place regarding a specific link.

The users who will receive this ticket are:

- The Approvers (entity managers) who approved or rejected the link.
- The Campaign Manager
- When the reviewed link involves a user, then the user is informed of the change.

All the info-tickets, for a specific event, provide the same information and functionality, independent of who receives them.

The ticket is marked by the icon ⓘ. After it is opened, the icon changes to ⓘ.

The ticket type is the same as the original Approver ticket (Delete Link [Entity1]-[Entity2]). But the functionality is limited.

In this section you will find information specific to the family of info-tickets.

<Ticket Title>

Delete Link [*Entity1*] [*Entity2*]. For example: Delete Link User-Resource.

Title

Request to remove [*Entity1*] to [*Entity2*] association. [*Entity1*]: [*Entity1-name*], [*Entity2*]: [*Entity2-name*]. For example: Request to delete role Organization=System Management (Characteristic Role (100.0%) - Min 40%) from user Angel Ben (67283470) - Approved and Completed Successfully.

Description

A description of the ticket. It includes the details of the request: Request was submitted on Universe [Universe name] from [Campaign Title]. For example: The request to delete role Organization=System Management (Characteristic Role (100.0%) - Min 40%) from user Angel Ben (67283470) was approved and completed successfully - Request was submitted on Universe Portal from Link of Team to Role(s).

Use this ticket's functionality when you wish to transfer the specific info-ticket to the management or attention of another user. You can use the options in the ticket's Advanced section to access additional information concerning the current ticket.

More information:

The Ticket Properties Form (see page 67)

General Approval Process Info-Ticket Functions

The Rejected-Link Parent ticket provides the following General functionality:

Close

Closes the info-ticket.

Save

Saves the changes made to the ticket.

Delegate

Transfers the info-ticket to another manager.

Escalate

Transfers the info-ticket to another manager.

Acknowledge

Click after reading the information provided by the info-ticket. The info-ticket is archived.

Click Acknowledge to end the process. The info-ticket is archived.

More information:

Delegate (see page 110)
Escalate (see page 108)

Advanced Approval Process Info-Ticket Functions

The Approval Process info-tickets provide 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.

Click any of the functions to access data connected with the info-ticket.

More information:

Add Comment (see page 70)
Add Attachment (see page 71)
View Transaction Log (see page 71)
View Parent (see page 113)
View Initiators (see page 113)

Chapter 10: How to Use 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

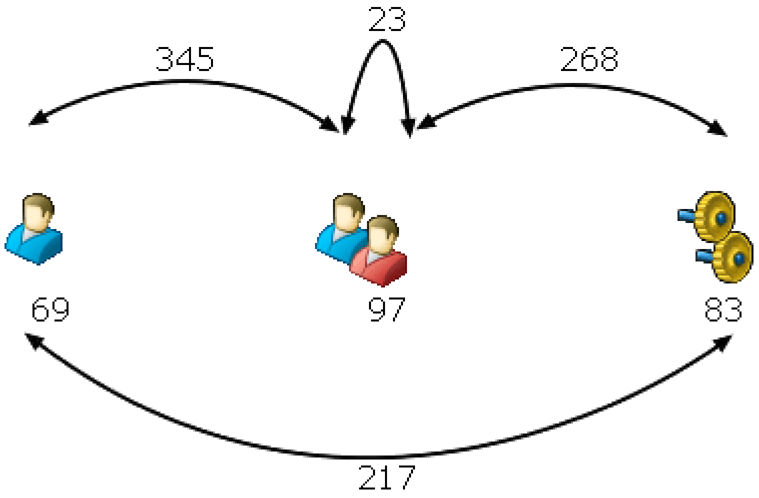
> Specifies if graphs show absolute values or percentages.

This section contains the following topics:

Configuration Dashboard

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 generated 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 11: 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 17), 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

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 137)
Suggesting Entities (see page 138)

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	■ 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 Mange My Team's Role Assignments on the Self-Service menu. The Manage My Team's Roles screen opens.

More information:

Customizing a Data Table (see page 19)
General Section (MMT-Role Screen) (see page 142)
Users Table (MMT-Role Screen) (see page 143)
Currently Enrolled Roles Table (Manage My Roles Screen) (see page 144)
Other Roles Table (MMT-Role Screen) (see page 146)

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:

Customizing a Data Table (see page 19)
Filtering a Data Table (see page 20)
Setting the Number of Records Per Page (see page 20)

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 ✕ to close the Violations window.
7. Click Submit.

   The Requests screen opens.

More information:

Approval Process Tickets (see page 105)
Filtering a Data Table (see page 20)
Setting the Number of Records Per Page (see page 20)
Customizing a Data Table (see page 19)
Test Compliance (see page 137)
Suggesting Entities (see page 138)
Introducing the Requests Table (see page 172)

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 Mange My Role Assignments on the Self-Service menu. The Manage My Roles screen appears.

More information:

Customizing a Data Table (see page 19)
General Section (Manage My Roles Screen) (see page 149)
Currently Enrolled Roles Table (Manage My Role Screen) (see page 150)
Other Roles Table (Manage My Role Screen) (see page 151)

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 150)
Other Roles Table (Manage My Role Screen) (see page 151)

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 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 151)

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 ✕ to close the Violations window.
6. Click Submit.

   The Requests screen opens.

More information:

Approval Process Tickets (see page 105)
Customizing a Data Table (see page 19)
Setting the Number of Records Per Page (see page 20)
Entity Card and Data Table Tabs (see page 21)
Test Compliance (see page 137)
Suggesting Entities (see page 138)
Introducing the Requests Table (see page 172)

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:

Customizing a Data Table (see page 19)
General Section (MMT-Resources Screen) (see page 154)
Users Table (MMT-Resources Screen) (see page 155)
Currently Enrolled Resources Table (Manage My Roles Screen) (see page 156)
Other Resources Table (MMT-Resources Screen) (see page 158)

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:

Customizing a Data Table (see page 19)
Setting the Number of Records Per Page (see page 20)
Filtering a Data Table (see page 20)
Currently Enrolled Resources Table (Manage My Roles Screen) (see page 156)
Other Resources Table (MMT-Resources Screen) (see page 158)

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 ✖ to close the Violations window.
6. Click Submit.

   The Requests screen opens.

More information:

Approval Process Tickets (see page 105)
Customizing a Data Table (see page 19)
Setting the Number of Records Per Page (see page 20)
Filtering a Data Table (see page 20)
Suggesting Entities (see page 138)
Test Compliance (see page 137)

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 Mange My Resource Assignments on the Self-Service menu. The Manage My Resources screen appears.

More information:

Customizing a Data Table (see page 19)
General Section (Manage My Resources Screen) (see page 161)
Currently Enrolled Resources Table (Manage My Resources Screen) (see page 162)
Other Resources Table (Manage My Resources Screen) (see page 162)

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:

Approval Process Tickets (see page 105)
Customizing a Data Table (see page 19)
Setting the Number of Records Per Page (see page 20)
Filtering a Data Table (see page 20)
Test Compliance (see page 137)
Suggesting Entities (see page 138)
Introducing the Requests Table (see page 172)

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 hierarchal 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 165)
Definitions for Role Name [New Role Name] (see page 169)

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:

Filtering a Data Table (see page 20)
Constructing a Rule (see page 168)
Definitions for Role Name [New Role Name] (see page 169)

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 165)
Filtering a Data Table (see page 20)
Customizing a Data Table (see page 19)
Suggesting Entities (see page 138)
Setting the Number of Records Per Page (see page 20)
Test Compliance (see page 137)
Introducing the Requests Table (see page 172)

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 165)
Filtering a Data Table (see page 20)
Request New Role Definition Screen (see page 165)
Definitions for Role Name [New Role Name] (see page 169)

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 ticket queue. 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 Ticket Queue.

More information:

Running Self-Service Tasks (see page 135)
Role Definition Tickets (see page 175)

Chapter 12: 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 (hierarchal) 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 theses 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

The Self-Service Approval Root-ticket is the root-ticket that appears in the ticket queue 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:

The Ticket Properties Form (see page 67)
Approval Root Ticket General Functions (Role Definition) (see page 181)
Approval Root Ticket Advanced Functions (Role Definition) (see page 182)

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' Ticket Queues.

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 108)
Delegate (see page 110)
Cancel Process (see page 117)
Acknowledge (see page 118)

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 70)
Add Attachment (see page 71)
View Transaction Log (see page 71)
View Children (see page 114)
View Statistics (see page 118)

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:

The Ticket Properties Form (see page 67)
Main Parent Ticket General Functions (Role Definition) (see page 184)
Main Parent Ticket Details Section (see page 184)
Main Parent Ticket Advanced Functions (Role Definition) (see page 185)

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 108)
Delegate (see page 110)
Cancel Process (see page 117)

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 processes 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 70)
Add Attachment (see page 71)
View Transaction Log (see page 71)
View Initiators (see page 113)
View Parent (see page 113)
View [Entity] (see page 115)

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 179)
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 184)

📄 Select Accountable	A Task ticket sent to the Self-Service task manager. For more information see Select Accountable Ticket (Add New Role) (see page 189).

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 193).

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 ticket	A Link Role-Resource parent 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 172)
Self-Service Request New Role Parent Ticket (see page 196)
Self-Service Request New Role Approver Ticket (see page 199)

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:

The Ticket Properties Form (see page 67)
Select Accountable (Function) (see page 190)
Select Accountable Ticket General Functions (see page 191)
Select Accountable Ticket Advanced Functions (see page 192)
View Violations (see page 193)

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:

Filtering a Data Table (see page 20)
Select Accountable Ticket General Functions (see page 191)

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 110)
Escalate (see page 108)
Select Accountable (Function) (see page 190)

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 70)
Add Attachment (see page 71)
View Transaction Log (see page 71)
View Parent (see page 113)
View Initiators (see page 113)
View [Entity] (see page 115)
View Violations (see page 193)

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 196)
Self-Service Request New Role Approver Ticket (see page 199)
Approve (see page 125)
Reject (see page 125)
Role Approver Ticket General Functions (see page 194)
Role Approver Ticket Advanced Functions (see page 195)

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 108)
Delegate (see page 110)
Approve (see page 125)
Consult (see page 123)
Reject (see page 125)

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 70)
Add Attachment (see page 71)
View Transaction Log (see page 71)
View Parent (see page 113)
View Initiators (see page 113)
View Violations (see page 193)
View Consult Results (see page 127)

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.

More information:

The Ticket Properties Form (see page 67)

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 108)
Delegate (see page 110)
Cancel Process (see page 117)

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 70)
Add Attachment (see page 71)
View Transaction Log (see page 71)
View Initiators (see page 113)
View Parent (see page 113)
View [Entity] (see page 115)
View Children (see page 114)

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 125)
Approve (see page 125)
New Role Approver Tickets' General Functions (see page 199)
New Role Approver Tickets Advanced Functions (see page 200)

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 110)
Escalate (see page 108)
Consult (see page 123)
Approve (see page 125)
Reject (see page 125)

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 70)
View Transaction Log (see page 71)
Add Attachment (see page 71)
View Initiators (see page 113)
View Parent (see page 113)
View [Entity] (see page 115)
View Consult Results (see page 127)

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 (see page 115).
📂 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 205)

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 305)
Updating Role Definitions (see page 171)
Running Self-Service Tasks (see page 135)
Manage My Team's Role Assignments (see page 141)
Self-Service Request New Role Parent Ticket (see page 196)
Self-Service Request New Role Approver Ticket (see page 199)

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.

More information:

The Ticket Properties Form (see page 67)

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 110)
Escalate (see page 108)
Cancel Process (see page 117)

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 70)
View Transaction Log (see page 71)
Add Attachment (see page 71)
View Parent (see page 113)
View Initiators (see page 113)
View Children (see page 114)
View [Entity] (see page 115)

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 196)
Self-Service Request New Role Approver Ticket (see page 199)
Approve (see page 125)
Reject (see page 125)
Update Role Approver Tickets' General Functions (see page 206)
Update Role Approver Tickets Advanced Functions (see page 207)

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 108)
Delegate (see page 110)
Consult (see page 123)
Approve (see page 125)
Reject (see page 125)

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 70)
Add Attachment (see page 71)
View Transaction Log (see page 71)
View Initiators (see page 113)
View Parent (see page 113)
View [Entity] (see page 115)
View Violations (see page 193)
View Consult Results (see page 127)

Chapter 13: Entity Browser

The Entity Browser enables you to locate any entity associated with any available Universe and configuration. Entities are:

- Users
- Roles
- Resources.

This section contains the following topics:

Main Window

The Entity Browser's main window provides you with a search option.

The search screen provides with two fields to aid in the search:

Universe

Provide the name of the Universe that you wish to search. You can select a specific Universe, limiting your choice of configuration, or you can select All.

Configuration

Select a configuration from the drop-down list.

After making your selection, the Entity Browser main window displays the search results.

The search results are presented using three tabs:

- Users
- Roles
- Resources

The standard operations available for all data tables are available here as well.

To obtain a specific list of entities

1. Click Entity Browser on the menu bar to open the search screen.
2. Select a Universe from the drop-down list
3. Select a Configuration from the drop-down list.

   The Loading bar is visible until the search results appear.

More information:

Entity Card and Data Table Tabs (see page 21)
Setting the Number of Records Per Page (see page 20)
Customizing a Data Table (see page 19)
Filtering a Data Table (see page 20)

Specific Entity browser

Once you have selected the configuration from which to obtain the entity data, the Entity Browser presents the information under three tabs:

- Users
- Roles
- Resources

The active tab is highlighted and the table contents can be manipulated.

Each specific entity tab can be manipulated independently of the others. For example, you can set the number of records per page for the Users tab to 50, and this will not change the number of records per page viewed in the Roles tab.

More information:

Users Browser (see page 211)
Roles Browser (see page 211)
Resources Browser (see page 212)
Data Table Features (see page 19)

Users Browser

The Entity Browser opens by default in the Users tab.

The Entity Browser’s Users tab shows user information for the selected configuration. The data and the field names are obtained from the configuration’s user database (*.udb).

Note: The highlighted column is predefined and cannot be customized.

You can click the highlighted Person ID in any record to open that user’s User Card.

To see the user's CA RCM portal user account information, click the Show in permissions configuration link. The Users tab the user's privileges in the CA RCM portal.

More information:

User Card (see page 23)

Roles Browser

Click on the Roles tab to open the Roles Browser.

The Entity Browser’s Roles tab shows role information for the selected configuration.

Note: The highlighted column is predefined and cannot be customized.

You can click the highlighted Role Name in any record to open that role’s Role Card.

More information:

Role Card (see page 24)

Resources Browser

Click the Resources tab to view the Resources browser.

The Entity Browser's Resources tab shows resource information for the selected configuration. The data and the field names are obtained from the configuration's resource database (*.rdb).

Note: The highlighted column is predefined and cannot be customized.

You can click the highlighted Res Name 1 in any record to open that resource's Resource Card.

More information:

Resource Card (see page 25)

Chapter 14: 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 214)
2. Select data files, specify customization parameters, and generate the report.	Parameters and Filters for Report Generation (see page 215)
3. View the report in your browser.	Display a Report's Index (see page 218)and Change Report Parameters (see page 218)
4. Export the report to a file, or print it.	Export a Report to a File (see page 218)or Print a Report (see page 219)

This section contains the following topics:

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.utils.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 TOC. 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 15: 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:

Adding Campaigns

Campaigns utilize CA RCM's basic auditing tools to run an enterprise wide certification and attestation process with the aid of 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.

A campaign runs a general corporate auditing process to determine the measure of the corporate compliance with various regulatory requirements on one hand, and with internal policies on the other. The campaign parameters are set by the administrator running the campaign. This administrator (also known as the campaign-owner) determines the universe on which the auditing process will be run; which policies will be examined and several other aspects of the campaign.

The campaign directs the auditing process, setting it to either basic role-based auditing or policy compliance auditing. By determining the campaign universe, the administrator who is the campaign-owner determines which configuration files will be audited.

The campaign-owner is responsible for creating the campaign and must generate or verify the existence of:

- The Universe in which the campaign will run.
- The RACI permissions for this Universe.

The campaign analyzes the user information in the context of the links between the users, roles and resources defined for the corporation. A campaign can focus on the links from the various viewpoints creating *User Campaigns* which focus on the users and their links, or *Role Campaigns* which focuses on the roles and their links, or *Resource Campaign* which focuses on the corporate resources and their links. Each campaign is defined for a specific viewpoint.

A campaign is completed either when all the approvers have approved/rejected the items they manage, or when the campaign-owner decides to arbitrarily stop the campaign.

The default workflow entails first running a campaign and collating all the rejected links, and only afterwards are those links actually reviewed and either they are rejected (severed) or they are approved in spite of the problem that caused them to be rejected during the campaign.

The Add Campaign screen contains the following fields:

Campaign Name

Defines the name of the campaign. Provide a unique and meaningful name.

Owner, Date Created

These fields are automatically completed by CA RCM.

Description

Defines a short description of the campaign.

Due Date

Specifies the target date for completion of all the campaign processes. Beyond this date, the campaign is shown in your ticket queue as overdue.

Universe

Specifies the universe on which the campaign is based.

Configuration

Specifies the configuration on which the campaign is based. The drop-down lists only configurations associated with the selected universe.

Note: You cannot select the active model configuration of the universe. You can base the campaign on a copy of the model configuration. The model configuration is cloned when the campaign is created.

Audit Card

(Optional) Specifies an audit card to include in the campaign. Violations from the audit card are indicated in approver tickets. The drop-down lists only audit cards associated with the selected configuration.

Privileges to Certify

Specifies the types of links that are included in the campaign: direct, dual, or indirect (see page 228).

Campaign Type

Specifies the type of campaign.

User

Approvers certify the roles and resources linked to the users under their management.

Role

Approvers certify the users and resources linked to the roles under their management.

Resource

Approvers certify the roles or users linked to the resources under their management.

Use Links

(Optional) Specifies filtering of reviewed links based on the specified audit card.

Only from audit card

Include only users and links that have violations listed in the Audit Card.

Only not in audit card

Include only users and links that do not appear in the AuditCard. This option is useful when the audit card contains approved violations.

Automatically provision campaign permissions

(Recommended) Override the eurekify.cfg permissions, in order to ensure that campaign-designated approvers are permitted access to the subjects of their approval. Select to ignore the system permissions and automatically provision campaign permissions. For example, this shortcut is useful as it allows managers to view tickets that otherwise they wouldn't be allowed to view because the security administrator had to run a campaign, even though the corporation is in the middle of setting up permissions. When this option is disabled, an Approver may receive a ticket, yet the ticket will be empty if the permissions were not defined so as to allow this Approver to view the relevant links.

Aggregate Approval Proces

Specifies whether changes are approved on a rolling basis, or collected into a distinct approval phase.

Don't wait for ticket processing (receive email when finished)

Select to enable processing of the campaign in the background. When a ticket is generated, you will receive email notification. For very large campaigns, have the system process the campaign creation offline (the campaign-owner can continue with other tasks), and send an email to the campaign-owner once the campaign has been created.

Generating a campaign is a resource intensive process, especially as the number of links is not limited to the number of system users. For example, in a company with 10,000 employees, and assuming each user has an average of 10 links (to resources and roles), you will have a campaign that requires the processing of approximately 100,000 links in order to create the campaign's tickets.

When this option is disabled, you will see a progress bar that shows the percentage of progress at any moment.

Auto Start

Specifies when the campaign is activated.

Disabled

The campaign is created but not activated. You must launch the campaign from your ticket queue.

Immediate Start

The campaign is created and launched when you click Create the Campaign on this screen. Tickets and emails are sent to all campaign participants.

Start at Specific Date

Schedule campaign launch for a future date and time. The campaign launch appears in the portal's job scheduler screen.

To add a campaign

1. On the Administration menu click Add Campaign.

   The Add Campaign screen opens.

2. Provide a unique Campaign name.
3. Enter a Description.
4. In the Due date box, enter a date or click the calendar icon and select a date.
5. In the Universe list, type or select a universe.
6. In the Configuration list, type or select a configuration.
7. (Optional) In the Audit Card list, select an audit card.
8. In the Campaign Type list, type or select a campaign type.
9. Select the relevant Privileges to Certify check boxes (Direct; Dual; Indirect). Clear the check boxes you want to disable.
10. (Optional) Select the Only use links from audit card check box.
11. (Optional) Select the Only use links not in audit card check box.

    Note: Be sure to select either Only user links from audit card check box or the Only use links not in audit card check box. You can select to ignore both options, but you cannot enable both.

12. (Recommended) In the Permissions section, select the Automatically provision campaign permissions check box.
13. (Optional) Advanced Settings may be available depending on portal configuration:
    - Select the Aggregate Approval Process (see page 230) checkbox to consolidate all approval tasks.
    - If customized workflows are enabled in the portal, you can select customized campaign processes. One alternative set of processes supplied with CA RCM is the bypass approval processes (see page 231) that skip approval tasks.
14. (Optional) Select the Don't wait for ticket processing check box.
15. In the Auto Start field, choose an option.
16. Click Create the Campaign.

The campaign is created and a ticket is generated in your queue. If the Don't wait for ticket processing option has been disabled, you will see a percentage progress bar on screen and when the campaign ticket is ready the Campaign Setting Completed screen opens.

This screen signals that the campaign generation has been completed, and contains the following:

- Campaign name
- Campaign type
- Universe
- Configuration
- Audit Card
- Number of approvers - as generated according to the RACI model
- Number of [entities] - total number of users, roles or resources that the approvers have to approve, depending on the campaign's focus.
- Campaign ticket ID

If the Don't wait for ticket processing option is enabled, the following message appears:

Your request was sent to execution, an email message will be sent upon completion.

Note: Any entity that does not have a manager will be assigned to the campaign administrator's approver ticket.

If you selected the Disable auto-start option, you must launch the campaign from your ticket queue.

More information:

Setting a Universe (see page 235)
Audit Cards (see page 228)
“Privileges to Certify” Options (see page 228)
Campaign Approver Tickets (see page 95)

“Privileges to Certify” Options

CA RCM identifies three types of links:

- Direct links
- Indirect links
- Dual links

You can select to examine one or more types of links during your campaign.

Direct Links

Refer to an immediate connection between entities. This is the most often examined type of link, and the most important.

Indirect Links

Refer to a link that goes through an intermediary. For example, a role is linked directly to both a resource and a user. There is no direct link between the user and the resource. The link between the user and the resource is an indirect link. Indirect Links can be reviewed, but they cannot be audited. A campaign can list them for general knowledge, but an Approver cannot approve or reject such a link.

Dual links

Are cases where there is both a direct link, for example between a resource and a user, but there is also an indirect link going through a role. During a campaign, only the Direct link is audited. The Indirect link is listed for general knowledge.

Audit Cards

CA RCM provides a mechanism to identify and list suspicious users, roles and resources in six categories:

- Suspect entities
- Suspect connections
- Similar roles and role hierarchy
- Similar resources
- In/out of pattern entities
- Entities with many/few connections.

An Audit Card file can be generated via the CA RCM DNA client tool. For further information see the section on Audit Card Generation and Management in the *DNA User Guide*.

You can take advantage of Audit Cards and utilize them during a certification campaign by providing the name of the Audit Card in the Add Campaign screen.

In this case, the Audit Card provides a kind of overlay over the entities being certified, enabling the display of the current violations. The campaign entities are matched with the violations in the selected Audit Card, and for each such entity (or link) that is found to have a violation associated with it, the campaign presents the entity (or related entity – in case of link) in red, and the number of violations is displayed in red as well, in the Approver ticket’s entity link table in the Violations column.

For example, if there is a pattern-violation regarding a user (e.g. the user is "suspected as a collector"), or if there is a compliance violation for a user, who is not allowed to have both roles A and B, and yet it is found that the user is linked to both roles. Such a finding will cause the user name to appear in red in the campaign’s Approver ticket entity table.

You can click the violation number to display the relevant violations in a separate browser window. You can also apply the Audit Card to a campaign as a kind of filter which will place restrictions over which entity links are displayed in the Approver tickets, and which are not. In this case, in addition to selecting an Audit Card in the relevant field in the Add Campaign screen, you will also have to select one of the available options:

Only use links from Audit Card

> The Campaign Approver tickets will only display links that are listed in the Audit Card. This is very useful if you wish to run a campaign that reviews only links that have been determined to be violations of system rules.

Only use links not in Audit Card

> The Campaign Approver tickets will only display links that are not listed in the Audit Card. This is very useful when the Audit Card represents authorized violations, and by filtering them out, you are saving time as you do not want the approvers to re-examine and certify these links.

Alternatives for Campaign Approvals

Most certification campaigns involve two phases:

- **Review—**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 the role can access.
- **Approval—**If a link is rejected during the review phase, 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 trigger approval tasks, because they change the base configuration.

CA RCM offers several options for implementing the approval phase of a campaign:

- **Aggregate Approvals**— all approval tasks are saved until the campaign manager decides to initiate the approval stage. Aggregation creates a clear structure of distinct review and approval phases. Approval tasks and notifications are consolidated, simplifying the work of resource owners.
- **Bypass Approvals**—the approval phase is eliminated. CA RCM immediately implements in the base configuration all changes made during the initial review.

You choose these options when you create the campaign.

In addition, you can abort the approval process after the campaign is activated by choosing the Create Campaign Results Configuration option in the campaign ticket tree. This option saves the results of the review phase of the campaign to configuration files.

Aggregate Approval Processes

The Aggregate Approval Process option creates a clear structure of distinct review and approval phases. Approval tasks and notifications are consolidated, simplifying the work of resource owners.

Most certification campaigns involve two phases:

- **Review—**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 the role can access.
- **Approval—**If a link is rejected during the review phase, 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 trigger approval tasks, because they change the base configuration.

By default 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.

If you select the Aggregate Approval Process option when you create a campaign, all approval tasks are saved until the campaign manager decides to initiate the approval stage. Only then are approval-related tickets activated and email notifications sent.

The following allowModifiedCampaign system property controls approval aggregation:

allowModifiedCampaign

Specifies if the Aggregate Approval Process check-box is available in the Add Campaign screen.

True

Makes the Aggregate Approval Process option available.

False

Hides the Aggregate Approval Process option.

To aggregate approval processes

1. Verify that the value of the allowModifiedCampaign system property is True.
2. When you define a new campaign, select the Aggregate Approval Process check box in the Advanced Settings section of the Add Campaign screen.

Bypass Approval Processes for a Campaign

Most certification campaigns involve two phases:

- **Review—**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 the role can access.
- **Approval—**If a link is rejected during the review phase, 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 trigger approval tasks, because they change the base configuration.

You can bypass the approval process. CA RCM immediately implements in the base configuration all changes made during the initial 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 campaigns that are based on a copy or subset of configuration data. Do not use this option with campaigns that are based on the active universe or an original version of a configuration file.

The following allowModifiedCampaignProcess system property controls this option:

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.

To bypass approval processes for a campaign:

1. Verify that the value of the allowModifiedCampaignProcess system property is True.
2. Copy a configuration file or create a partial file containing relevant data.
3. In the Settings area of the Add Campaign screen, define a new campaign. Specify the data file you created as the base for the campaign. Do not specify an active universe, or the original version of a data set.

   The Remove Link processes used by the specified type of campaign are shown in the Advanced Settings area.
4. 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.
   - Select the regular version of the process to trigger approval tasks when that type of link is rejected.
5. Complete other campaign settings, and click Create the Campaign.

Campaigns Based on the Active Model Configuration

Every universe has two basic configurations: master and model. The master is a reference configuration. The model is constantly updated by data import and role modeling processes.

Often, you want to base a campaign on the active 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 Add Campaign screen.

The following system properties control campaigns that reference the active model configuration:

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.

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

Start Approval Process from DNA

There is a possibility to create an AuditCard in the CA RCM DNA module that reflects changes between two configurations (the pre-configuration and the post-configuration, along the lines of master and model), 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. The former two types always appear in the ticket queue as In Process and hence Start Process is disabled.

Setting a Universe

A universe refers to a specific Master-configuration and Model-configuration pair that includes the entitlements of one or more end-points.

- 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 as the audit process proceeds, the model-configuration is updated based on the corporate policies and regulatory compliance demands.

CA RCM Portal permissions are derived from the universe definition.

Note: Once you have defined a universe, you have to run the CA RCM Configuration settings utility so that the users can access the CA RCM Portal.

You also have to generate the RACI configuration, to define the entity Approvers.

This section describes the following procedures:

- Access the Universe Settings List
- Create a new universe
- Edit a universe
- Delete a universe

More information:

CA RCM Configuration Settings (see page 274)
RACI Operations (see page 275)
The Universe Settings Table (see page 236)
Creating a New Universe (see page 236)
Editing a Universe (see page 239)
Deleting a Universe (see page 239)

The Universe Settings Table

The Universes table displays a list of available universes, their description and the options of editing or deleting an existing universe. A Create New button allows you to generate a new universe.

#

The universe's ID number.

Name

The universe's name.

Description

The universe's description.

Edit

Provides the option of editing the universe definitions.

Delete

Provides the option to delete a universe.

To access the Universe settings table

1. On the Administration menu click Settings.

   The available options list appears:

2. Click Universe Settings.

   The Universe list appears.

Creating a New Universe

It is recommended that you create a new universe the first time you run the CA RCM Portal. You will use this universe in order to run the first import and audit procedures. Sometimes, it is necessary to create a separate universe for specific purposes, for example when running an audit on a partial configuration.

As a universe contains a specific master/model configuration pair, you can either use real configuration names, if you already have them, or you can use names that will be “place-savers” and can be replaced in the future when you know the true configuration file names. When you aren't referring to an existing configuration, the information fields will have to remain empty during the creation of the new universe. Make sure to fill in the information prior to running a campaign based on this universe.

Note: If the configuration files do not exist, the Import process will create them.

The Create New Universe screen contains the following fields:

Universe Name

Provide the name of the universe.

Description

Provide a description of this universe (its use, the type of configuration used etc.)

Master configuration name

The Universe's master configuration. The file name has to have the extension .cfg. If the configuration was uploaded to the database, the name will appear in the autocomplete list.

Model configuration name

The Universe's model configuration. If the configuration was uploaded to the database, the name will appear in the autocomplete list.

Approved Audit Card

The list of approved violations for the Universe (if it exists).

Configuration Login field

The field, in the selected configuration file, which provides the users' login ID (located in the users database file).

Configuration email field

The field, in the selected configuration file, which provides the users' email address (located in the users database file).

Configuration user manager field

The field, in the selected configuration file, which provides the user manager's ID (user approver).

Configuration role manager field

The field, in the selected configuration file, which provides the role manager's ID (role approver).

Configuration resource manager field

The field, in the selected configuration file, which provides the resource manager's ID (the resource approver).

Audit Settings file

Parameters and settings which define the audit and pattern-based checks that will be performed on the master configuration each time it's imported.

Important! Each Universe has a unique configuration associated with it. Do not create more than one universe for any master/model configuration.

To create a Universe

1. On the Administration menu click Settings.

   The list of available options appears.

2. Click Universe Settings.

   The Universe list appears, displaying existing universes.

3. Click Create Universe.

   The Create New Universe screen opens.

4. Provide a unique Universe Name and Description.

5. Provide a unique Master configuration name.

   Note: We recommend that when generating a new Universe that you use the terms Master/Model as part of the configuration file names. For example: Master_configWithRoles.cfg and Model_configWithRoles.cfg respectively.

6. Provide a unique Model configuration name.

   The remaining fields depend on the existence of the configuration provided.

   Note: If the configuration exists, and it is located in the database, the CA RCM Portal autocomplete feature will allow you to select content from a list of options for each field.

7. (Optional) Select an Audit settings file from the drop-down list.

8. Click Save. The universe is created and will appear in the Universe List.

   Note: Sometime an issue exists (for historical reasons) that causes a message to appear. At the bottom of the message you are asked if you want to auto-repair the issues in this message. Always click Yes.

9. 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.

After you have created a new universe, you need to perform the following actions:

- Update CA RCM users' database
- Create RACI
- Sync RACI

More information:

Monitor the First Run of a Connector (see page 248)
CA RCM Configuration Settings (see page 274)
Create RACI (see page 275)
Synchronize RACI (see page 276)

Editing a Universe

To edit an existing Universe

1. Click Edit next to the Universe that you want to edit. You cannot change the name of a universe. The contents of the other fields can be edited.

   Note: We recommend that when editing a universe's configuration file names, make sure that the configurations were not assigned to another universe.

2. Click Save.

   Note: Sometime an issue exists (for historical reasons) that causes a message to appear. At the bottom of the message you are asked if you want to auto-repair the issues in this message. Always click Yes.

3. 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.

Deleting a Universe

To delete a Universe

1. Click Delete next to the Universe you want to edit.

   A confirmation message appears.

2. Click Yes to delete the universe.

Setting Connectors to Import and Export Data

Connectors are defined for specific converters, which are service programs necessary for importing and exporting user and user privileges information (entities and the links between them) from corporate security systems into CA RCM. Import/Export processes can be performed either from the CA RCM Data Management (DM) client tool or through the CA RCM Portal.

User and user privileges information can be imported directly into CA RCM by using the Import option on the CA RCM Data Management (DM) menu bar (see Chapter 2: in the CA RCM Data Management manual). This option enables importing Active Directory, CSV, RACF or SQL files into CA RCM by creating a communications link to the downloading (production) server. CA RCM Sage database files are simple text files. However, CA RCM converters ensure that imported files will adhere to CA RCM Sage file format rules.

The DM module provides a number of converters. Each converter supports a specific type of data source. There are three basic types of data sources:

Platform specific

These converters enable the download/upload of information stored in the native security systems on the most common operating systems (for example: UNIX or SAP).

Specialty security systems (for example: RACF)

This refers to security-dedicated software systems located on various platforms.

Identity management systems (for example CA Identity Manager)

This refers to human resource software systems located on various platforms.

The CA RCM Portal provides you with the option to define these converters as Import Connectors or Export Connectors for the specific corporate environment. The converters are conveniently located in the Import and Export menus of the CA RCM Data Management application. For further information on importing, exporting and converters see the *Data Management User Guide*.

Note: At some point you may have to access the DM in order to edit the specific converter's Settings and Mappings file. For further information see the *Data Management User Guide*.

At the end of an audit process, the original configuration that was downloaded from the end-point is compared to the new configuration. The configuration variance between the original and the updated configuration, resulting from the audit and the implementation of corporate policies and enforcing regulatory compliance, is uploaded via Export-Connectors to the endpoints.

This section discusses the following procedures:

- The Connector Settings panel
- Create a new import connector
- Create a new export connector
- Run a connector
- Edit a connector
- Delete a connector

Connectors are defined specifically either as an import connector or as an export connector.

More information:

The Connector Settings Panel Tables (see page 241)
Creating a New Import Connector (see page 241)
Creating a New Export Connector (see page 244)
Monitor the First Run of a Connector (see page 248)
Import Error Tickets (see page 250)

The Connector Settings Panel Tables

The Connector Settings panel provides two connector tables:

- Imports
- Exports

Each table displays a list of available connectors, ID numbers description and provides the options to Edit, Delete or Run a connector. The Create New button, located above each table, allows you to generate a new import connector or a new export connector.

To access the connector tables

1. On the Administration menu click Settings.

   The list of available options appears.

2. Click Connector Settings. The Connector Settings screen opens.

To edit an existing connector

1. Click Edit next to the connector that you want to edit. You cannot change the name of a connector. The contents of the other fields can be edited.

To delete a connector

1. Click Delete next to the connector that you want to delete.

   A confirmation prompt appears.

2. Click OK to delete the connector.

Creating a New Import Connector

Connectors utilize the CA RCM converters to import data from the system's endpoints. You will need to know which converter you intend to use and the name and location of the settings (xml) file and the mapping (xml) file for this converter. For more information see the *Data Management User Guide.*

Import client name

Provide a name for the import connector.

Description

Provide a description of the import connector (its use, timing etc.)

Universe

Provide the name of the universe to be associated with this import connector. The data obtained through this connector will be downloaded into the universe's master configuration files. In the case of a first time download, and there are no pre-existing configuration files, the import process will create the configuration files.

Note: Before you can run a connector job, you must explicitly declare a login field for the universe, and verify that the connector maps endpoint data to this field.

Settings XML file

Create this file in the CA RCM DM module. It is usually located in the directory <CA RCM Home Directory>\<Converter Directory>. The installation provides a default *defaultsettings.xml* file. For more information see the *Data Management User Guide.*

Mapping XML file

Create this file in the CA RCM DM module. It is usually located in the directory <CA RCM Sage Home Directory>\<Converter Directory>. The installation provides a default *mapping.xml* file. For more information see the *Data Management User Guide.*

Enrichment settings file

(Optional) The data is usually downloaded from a specific endpoint. 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 you can then enrich the data by accessing additional data from a human resources database. This data may include, for example, user addresses which were not available from the primary source of information. For further information see Chapter 4 of the *Data Management User Guide.*

Remote system login password

The password is not saved within the system settings. Provide it at this point.

Max duration time (seconds)

Provide an estimate of how long the import process takes. This is useful when you know how long it should take, and therefore a longer import time, indicates that there is a problem. You do not have to know exactly how long it takes. You can provide an estimate. The import process will end when the time specified is over.

Connector Java Class

Select the Java Class that matches the converter you will be using to import the data from the system's endpoints. Sbt* classes enable the connection between the CA RCM Portal which was written in Java and the CA RCM DNA which is not.

Workflow process name

Select the default import process. You can use the bundled Workpoint™ BPM engine to generate additional workflow processes.

Ticket Type

Tickets are work items that can be viewed in the Ticket Queue. Select the default ticket type.

Priority

Set the priority level. The available options are:

- Low
- Normal
- Rush
- Critical

Severity

Set the severity level. The available options are:

- Minimal
- Medium
- Serious
- Urgent
- Critical

To create a new Import Connector

1. In the Connector pane, click Create New.
2. Enter the name of the new Import Connector.
3. Provide a clear and concise Description of the import connector.
4. Select the Universe from the drop-down list.
5. Enter the name and location of the Settings XML File.

   You have to provide the full path and file name. You can locate the file using your systems file browser and copy the name and path from the Address bar and paste it in the text box.
6. Enter the name and path of the Mapping XML File.

   You have to provide the full path and file name. You can locate the file using your systems file browser and copy the name and path from the Address bar and paste it in the text box.
7. (Optional) Provide the name and path of the Enrichment Settings file.
8. Enter the Remote system login password for accessing the endpoint.
9. Provide an upper estimate (in seconds) for the Max duration time.
10. Select the appropriate converter's Connector Java Class.
11. Select the default Workflow process name.
12. Select the default import Ticket Type.
13. Select the Priority.
14. Select the Severity.

When the new import connector is created, it appears in the Imports table.

More information:

Tickets and the Ticket Queue (see page 55)

Creating a New Export Connector

Connectors utilize the CA RCM Sage converters to export data to the system's endpoints. You will need to know which converter you intend to use and the name and location of the settings (xml) file and the mapping (xml) file for this converter. For further information see the *Data Management User Guide.*

Export client name

Provide a name for the export connector.

Description

Provide a description of the export connector (its use, timing etc.)

Universe

Provide the name of the universe to be associated with this connector. The uploaded data will be based on the universe's master/model configuration files.

Settings XML file

Create this file in the DM module. It is usually located in the directory <CA RCM Sage Home Directory>\<Converter Directory>. For further information see the *Data Management User Guide.*

Mapping XML file

Create this file in the DM module. It is usually located in the directory <CA RCM Sage Home Directory>\<Converter Directory>. For further information see the *Data Management User Guide.*

Remote system login password

The password is not saved within the system settings. Provide it at this point.

Max duration time (seconds)

Provide an estimate of how long the export process takes. This is useful when you know how long it should take, and therefore a longer export time, indicates that there is a problem. The export process will end when the specified time is over.

Connector Java Class

Select the Java Class that matches the converter you will be using to import the data from the system's endpoints. Sbt* classes enable the connection between the CA RCM Portal which was written in Java and the CA RCM DNA which is not.

Workflow process name

Select the default export process. You can use the bundled Workpoint™ BPM engine to generate additional workflow processes.

Ticket Type

Tickets are work items that can be viewed in the Ticket Queue. Select the default export ticket type.

Priority

Set the priority level. The available options are:

- Low
- Normal
- Rush
- Critical

Severity

Set the severity level. The available options are:

- Minimal
- Medium
- Serious
- Urgent
- Critical

To create a new export connector

1. In the Connector pane, click Create New.
2. Enter the name of the new Export Connector.
3. Provide a clear and concise Description of the export connector.
4. Select the Universe from the drop-down list.
5. Enter the name and location of the Settings XML File.

   You can locate the file using your systems file browser and copy the name and path from the Address bar and paste it in the text box.
6. Enter the name and path of the Mapping XML File.

   You can locate the file using your systems file browser and copy the name and path from the Address bar and paste it in the text box.
7. Enter the Remote system login password for accessing the endpoint.
8. Provide an upper estimate (in seconds) for the Max duration time.
9. Select the appropriate Connector Java Class.
10. Select the default Workflow process name.
11. Select the default import Ticket Type.
12. Select the Priority.
13. Select the Severity.

When the new export connector is created, it appears in the Connector Settings Exports table.

Data Enrichment of New User Accounts

During data import, you can have CA RCM 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, you specify this 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 275) 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.

Run or Schedule a Connector Job

You can run predefined connector jobs to exchange data with external provisioning platforms.

To run or schedule a connector job

1. Log in to the CA RCM portal as an administrator.
2. Click Administration, Settings, Connector Settings.

   The Connector Settings screen appears.
3. Select *one* of the following options:
   - Click Run adjacent to the job profile you want to run.

     The job begins immediately.
   - To schedule future execution of a job, click Schedule.

     The New Connector Scheduled 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. The connector job runs at the scheduled times.

Monitor the First Run of a Connector

You define new configuration files for the connector to use, and specify the data field that is mapped to create a CA RCM portal login for new users. You can perform these tasks manually, but it is simpler to run the connector job and perform these tasks through the job ticket. Follow this procedure the first time you run an import/export connector from the CA RCM portal.

To monitor the first run of a connector

1. Click Ticket Queue on the portal main menu.

   Your ticket queue appears.

2. If the queue contains an Error Handling ticket for the connector job:

   a. Double-click the Error Handling ticket.

      The Ticket Properties Form dialog opens.

   b. Open the More section of the form.

      An error message indicates that Master and Model configurations do not exist in the target universe.

   c. Click Handle.

      The Create Universe button appears.

   d. Click Create Universe.

      The error is resolved.

   e. Close the ticket.

3. In the ticket queue, click Refresh.

4. If the queue lists a new Error Handling ticket:

   a. Double-click the Error Handling ticket.

      The Ticket Properties Form dialog opens.

   b. Open the More section of the form.

      An error message indicates that the required LoginID field has not been mapped to a field in the retrieved data.

   c. Click Handle.

      The Skip Synchronization button appears.

   d. Click Skip Synchronization.

      The error is resolved.

   e. Close the ticket.

5. In the ticket queue, verify that the connector job proceeds.

   Note: You can open the connector ticket to monitor the progress of the job.

More information:

Job Scheduling (see page 258)
The Ticket Properties Form (see page 67)
Delegating an Info-Ticket (see page 74)
Escalating an Info-Ticket (see page 75)

Import Error Tickets

When an import operation fails for some reason, 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

The button is disabled until the process is completed. Click to complete and archive the ticket.

Handle

This button ensures that even 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.

Clean up

Cleans up the job's temp files prior to terminating the job.

More information:

The Ticket Properties Form (see page 67)
Delegating an Info-Ticket (see page 74)
Escalating an Info-Ticket (see page 75)

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.

There are two steps to implement a multi-import job:

1. Define a multi-import job (see page 251) and each of its connectors on the portal.
2. Run or schedule (see page 258) this multi-import job using the job scheduling tools of the portal.

When it merges data from several sources, the multi-import process reconciles the data mappings of the various sources. The resulting configuration file may not match the data scheme of existing configurations in the universe.

- If you use multi-import to populate a new, empty universe (see page 257) the merged configuration defines the default data scheme of the universe. This is the most common use of multi-import.
- If you use multi-import to import data into an existing universe, you must verify that all the data sources have data mappings that match each other and the universe.

Define a Multi-Import Job

You define a multi-import job on the portal. You can run this job to import data from several sources automatically.

To define a multi-import job

1. Log in to the CA RCM portal as an administrator.
2. From the main menu, click Administration, Settings, Multi Import.

   The Multi Imports main screen appears.
3. Click Create 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.

6. Add an import task to the multi-import job:

   a. Select the type of import job you want from the Select Connector Import Implementation drop-down, and click Configure & Add to Merge.

      A configuration screen appears. Fields for the type of import job you selected are listed.

   b. Enter values to define the import job.

      Note: Some import job options are not available, such as data enrichment.

   c. Click Done.

      The new import task appears in the table.

   Repeat these steps to define as many import tasks as you want.

7. (Optional) Click Delete in the row of an import task to remove it from the job.

8. Set the completion level for the job:

   a. Click Manage Groups.

      The Manage Group window appears.

   b. Click Edit to edit the default group.

      The Group window appears.

   c. Edit the following field:

      - **Completion Level—**
      - Defines the percentage of import tasks that must complete successfully for the multi-import job to be considered 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).

   d. Click Save twice.

      The completion level is set for the job.

9. In the Multi Import editing screen, click Save.

   The Multi Imports main screen appears. The new multi-import job is listed in the table.

More information:

Define a CSV file Import Connector (see page 253)
Define a Configuration Import Connector (see page 254)
Define an Import Connector for CA Identity Manager r12.0 and Earlier (see page 255)

Define a CSV file Import Connector

To import data from a set of comma-separated values (CSV) files, define a CSV file import connector. You can also use this connector to import from files that use another character to separate data values.

To define a CSV file import connector

1. In the multi import editing screen, select CSV Files Import Connector from the Select Import Connector Implementation drop-down. Click Configure and Add to Merge.
2. The Import Connector: CSV Files Import Connector screen appears.
3. Enter values in the Name and Description fields of the connector.
4. Enter values for the following required fields:

   usersFile

   Defines the pathname of the CSV file that contains user data.

   rolesFile

   Defines the pathname of the CSV file that contains role data.

   resourcesFile

   Defines the pathname of the CSV file that contains resource data.

   targetConfigurationName

   Defines the configuration file that receives imported CSV data.

   The user, role, and resource entities in these files are imported into the specified configuration file. If this connector is part of a multi import job, this configuration file is merged with other import streams and integrated into the target universe of the multi import job.

   Note: The imported entities are not linked. For example, an imported role does not link to any resources, and no users are assigned to it.

5. (Optional) Enter values for any of the following fields to import link information:

   roleResourceLinksFile

   Defines the pathname of the CSV file that contains role-resource link data.

   roleRoleLinksFile

   Defines the pathname of the CSV file that contains role-role link data.

userRoleLinksFile

Defines the pathname of the CSV file that contains user-role link data.

userResourceLinksFile

Defines the pathname of the CSV file that contains user-resource data.

Link information from the specified CSV files is added to the configuration file.

6. (Optional) Complete the following fields to control details of the data import process:

   removeRedundantLinks

   Specifies if redundant links are removed during import.

   Values: True, False

   removeRstyle

   Specifies if the **\r** string is removed from the source files. CA RCM client tools insert this string when they create CSV files.

   Values: True, False

   removeDNAstyle

   Specifies if the \\ string is removed from the source files. CA RCM client tools insert this string when they create CSV files.

   Values: True, False

   customizedSeparator

   Defines the character that separates data values in the source files. Use this parameter to work with nonstandard files that do not use a comma character as a deliminator.

   customizedQuotechar

   Defines the character used as a quotation mark in the source files.

7. Click Done.

   The settings are saved.

Define a Configuration Import Connector

You can specify an existing configuration file as a data source for a multi import job. During multi import, data in the configuration is merged into the target universe.

To define a configuration import connector

1. In the multi import editing screen, select Database Configuration Files Import Connector from the Select Import Connector Implementation drop-down. Click Configure and Add to Merge.

2. The Import Connector: Database Configuration Files Import Connector screen appears.
3. Enter values in the Name and Description fields of the connector.
4. Select the source configuration in the Configuration drop-down field. CA RCM merges this configuration file with the other data streams of the multi import job.
5. Click Done.
6. The settings are saved.

Define an Import Connector for CA Identity Manager r12.0 and Earlier

Use this procedure to define a connector that imports endpoint data through CA Identity Manager.

Important! Configure connection, endpoint, and data mapping files before you use this connector. For detailed procedures, refer to the *Connector for CA Identity Manager Guide*.

To define an import connector for CA Identity Manager

1. In the multi import editing screen, select CA Identity Manager Import Connector from the Select Import Connector Implementation drop-down. Click Configure and Add to Merge.

   The Import Connector: CA Identity Manager Import Connector screen appears.

2. Enter values in the Name and Description fields of the connector.
3. Enter information in the following fields:

   CONF_FOLDER

   Defines the pathname to the server-side copy of the connector configuration files. Typically this pathname is the **/Connectors/Identity Manager/conf** directory, which you created on the server when you configured the connector.

   TARGET_CONFIGURATION_NAME

   Defines the target configuration file for data import. CA RCM adds new data entities to this file.

Settings XML file

Defines the pathname to the server-side copy of the connection settings files. Typically this pathname is the **/Connectors/CA/conf** directory you created on the server when you configured the connector.

Mapping XML file

Defines the pathname to the server-side copy of the connector data mapping file. Typically this pathname is the **/Connectors/CA/conf** directory you created on the server when you configured the connector.

Password

Defines the password used to log in to the target CA Identity Manager instance. CA RCM encrypts this value and saves it with the connector job.

4. Click Done.

   The settings are saved.

Use Multi-Import to Populate an Empty Universe

Multi-import is an ideal tool for building a new universe of CA RCM data. You can define and run a single job that automates the following processes:

- Imports data from several major provisioning nodes or other sources
- Reconciles field mapping across the data sources
- Merges data from the various import connectors
- Generates a configuration with a best-fit data scheme
- Populates the universe with the 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 interact with the process ticket in your ticket queue to create the master and model configuration files. This procedure describes these additional steps.

To use multi-import to populate an empty universe

1. Define a new universe on the CA RCM portal (see page 236). Specify dummy names for the master and model configurations. Do not use names of existing configurations.
2. Define a multi-import job (see page 251). Select the new universe you created.
3. Run the job (see page 258).
4. Click Ticket Queue on the portal main menu.

   Your ticket queue appears. It contains 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 your ticket queue 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

The Job Scheduling function enables you to set up automatic and repeated import/export instances. As each connector is assigned to a universe, the data will be imported into/uploaded from the CA RCM configuration files designated by the universe. An appropriate ticket is sent to the administrator's Ticket Queue when the job is completed.

The screen is divided into two sections:

Job Scheduling

Enter the relevant data in the fields in this section to create a new import/export event.

Jobs

A table listing all the recorded jobs and their description.

Run or Schedule a Job on the CA RCM Portal

You can run predefined connector jobs or other processes in the portal.

To run or schedule a job on the CA RCM portal

1. Locate the job or process you want to run.
2. Do *one* of the following:
   - To run the job immediately, click Run in the row of that process.

     The job begins immediately.

- To schedule one or more future jobs:

  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

  – **Number of 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

The name of the job.

Description

A description of what it does (export/import).

Job Class

Lists the connector's Java Class.

Start Time

Provides the date and time on which the job will begin.

Previous Execution

When a job is repeated, the previous date and time is listed here.

Next Execution

The date and time when the job is scheduled to be repeated.

Delete

Allows you to delete the job when you don't want it to run anymore.

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.

More information:

Setting the Number of Records Per Page (see page 20)

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.ConfigurationDashboar
dPage,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 272)

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 263)
Clear the Cache (see page 263)

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 that 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 271)
CA RCM Properties (see page 305)
Setting the Number of Records Per Page (see page 20)

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 271)
Editing a Property Key (see page 272)

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 permsisions 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 274)

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 247) 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:

Tickets and the Ticket Queue (see page 55)

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. The extracted data snapshot is a static copy of CA RCM objects. CA RCM does not update the data snapshot after it is created.

Extracted data is stored in a dedicated SQL database. Use the External Report Database option of the CA RCM installer to create this database.

You perform these procedures when you work with data extraction:

- Create an extraction profile (see page 279) that defines the types of data files that are copied to the external report database.
- Generate a data set, or snapshot (see page 280), 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 281). Data extraction jobs appear in the ticket queue of the administrator who runs/schedules them.
- Delete profiles and data snapshots (see page 282) 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.

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 ticket queue.

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 ticket queue. 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 Ticket Queue on the main toolbar.

   The Ticket Queue 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 theSnapshots 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 theSnapshots 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.

How to Work with IPv6

Internet Protocol version 6 (IPv6) is a new version of the Internet Protocol that supports 128-bit addresses.

In this release, not all components of CA RCM accept the extended IP addresses specified by IPv6. To implement CA RCM in an environment that uses IPv6 addresses, use host names instead of explicit IP addresses.

Servers can be mapped to host names in two ways:

- On the DNS in the operating environment.
- In the hosts file on each CA RCM computer.

Chapter 16: 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

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 286)
Authentication Settings (see page 287)
Encryption (see page 287)

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 288)

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 288)

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 290)

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 307)

Chapter 17: Troubleshooting

This chapter provides a list of the CA RCM Portal Error Messages

This section contains the following topics:

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 eurekify.properties
campaign.text.campagin.errors.found.errcode	cmp002	errors found
campaign.error.nouniversesavilable.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 then once
dashboard.compliance.error.nocard.errcode	dbc003	please enter all audit cards
dashboard.compliance.error.multicard.errcode	dbc004	auditcard {0} appears more then 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.errorgettingraciconfigurations. 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	tkt007	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	tkt008	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	tkt009	request to delete resource {1} from user {0} - rejected.
changeapproval.child.remove.user.resource.info .title.failed.errcode	tkt010	request to delete resource {1} from user {0} - failed.
changeapproval.child.remove.user.resource.info .description.rejected.errcode	tkt011	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	tkt012	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	tkt013	request to delete resource {1} from user {0} is already in process.
changeapproval.child.remove.user.resource .notification.description.errcode	tkt014	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	tkt015	request to add role {0} to role {1} - rejected.
changeapproval.child.add.role.role.info.title.faile d .errcode	tkt016	request to add role {0} to role {1} - failed.
changeapproval.child.add.role.role.info.descripti on .rejected.errcode	tkt017	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.descripti on .failed.errcode	tkt018	the request to add role {0} to role {1} failed - request was submitted on universe {2} from {3}
changeapproval.child.add.role.role.notification.til e .errcode	tkt019	request to add role {0} to role {1} is already in process.
changeapproval.child.add.role.role.notification .description.errcode	tkt020	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	tkt021	request to delete role {0} from role {1} - rejected.
changeapproval.child.remove.role.role.info.title.failed.errcode	tkt022	request to delete role {0} from role {1} - failed.
changeapproval.child.remove.role.role.info .description.rejected.errcode	tkt023	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	tkt024	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	tkt025	request to delete role {0} from role {1} is already in process.
changeapproval.child.remove.role.role.notification .description.errcode	tkt026	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	tkt027	request to add resource {1} to role {1} - rejected.
changeapproval.child.add.role.resource.info.title.failed.errcode	tkt028	request to add resource {0} to role {1} - failed.
changeapproval.child.add.role.resource.info .description.rejected.errcode	tkt029	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	tkt030	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	tkt031	request to add resource {1} to role {0} is already in process.
changeapproval.child.add.role.resource.notification .description.errcode	tkt032	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	tkt033	request to delete resource {1} from role {1} - rejected.
changeapproval.child.remove.role.resource.info.title .failed.errcode	tkt034	request to delete resource {0} from role {1} - failed.
changeapproval.child.remove.role.resource.info .description.rejected.errcode	tkt035	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	tkt036	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	tkt037	request to delete resource {1} from role {0} is already in process.
changeapproval.child.remove.role.resource .notification.description.errcode	tkt038	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	tkt039	to continue please choose an accountable user to {0} role
changeapproval.child.remove.user.role.notificati on .description.errcode	tkt094	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.checkjobticket exists.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.optimisticlockexceptio n .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.errc ode	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.missingdescripti on .errcode	ust003	missing description field.
settings.strings.universes.errors.namealreadyexi st .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.missingauditset tingsfile.errcode	ust007	was unable to find the audit settings file {0}.
settings.strings.universes.errors.masterisnotread only .errcode	ust008	the master configuration ({0}) is not read only.
settings.strings.universes.errors.masterhasparen t .errcode	ust009	the master configuration ({0}) has a parent configuration.
settings.strings.universes.errors.masternotlogge d .errcode	ust010	the model configuration ({0}) is not logged.
settings.strings.universes.errors.modelisnotread only .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

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

```
 <?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.ConfigurationResourcesAttributesParamet
ersPage</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>
- <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>
- <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>Eurekfiy Configuration Settings</label>
  <checkPermission>false</checkPermission>
- <tag id="UpdateSagemaster">
  <type>internal</type>
  <label>Update Eurekfiy 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

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
- Additional fields (optional)
- Up to 6 additional fields per user

Example:

```
234A745,Tony O Smith,Sales US West Coast,Sales,San Francisco, 234A111, 5

373B234,Mark W Johnson,San Jose Wireless Research,R&D,San Jose, 123B546,1
```

Resource Database File

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
- Resource Name 2
- Resource Name 3
- Additional fields (optional)
- Up to 6 additional fields

Example:

```
System Administrator,Unix-348,Unix,AIX,ControlSA ESS

Marketing Managers,NT-720,NT,Windows,PR Planning
```

Configuration File

Each line in this file represents one entity and/or one relationship.

Reference to Static Users and Resource Databases.

This section comprises the first two lines in the file, and it provides a reference to the users and resource database files. These lines have the following formats:

```
UsersDB,<Users Database File Name>

ResDB,<Resource Database File Name>
```

Multiple configurations may share the same users and resource database files, even if only a small number of users and/or resources actually participate in each configuration.

Entities

This section describes the entities that participate in this configuration. The first set of lines identifies the users, one line per user, in the following format:

```
User,<CA RCM UserID>,<SA User ID>
```

The CA RCM User ID is used to describe the rank of the user in the users database file with the first number being “0” (thus, the fourth user in the database will have a CA RCM User ID of 3).

The second set of lines identifies resources, one line per resource, in the following format:

```
Res,<CA RCM Resource ID>,<User Group Name>,<Resource Name>,<Resource Type>
```

The CA RCM Resource ID is the rank of the resource in the resources database file (with the first number being “0”).

The third set of lines in this section identifies roles (if existing), one line per role, in the following format:

```
Role,<CA RCM Role ID>,<Role Name>,<Description>,<Organization>,<Owner>
```

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.

Relationships

This section consists of the following types of line formats:

User - Resource Permission

```
User-Res,<CA RCM Sage User ID>,<CA RCM Sage Resource ID>
```

User - Role Permission

```
User-Role,<CA RCM Sage User ID>,<CA RCM Sage Role ID>
```

Role - Resource Permission

```
Role-Res,<CA RCM Sage Role ID>,<CA RCM Sage Resource ID>
```

Role Hierarchy Permission

```
Role-Role,<CA RCM Sage Role ID of parent role>,<CA RCM Sage Role ID of child role>
```

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