CA Identity Governance

Administration Guide

12.6.02a

CA Technologies Product References

- This document references the following CA Technologies products:
- CA Identity Governance
- CA Identity Manager
- CA SiteMinder®
- CA User Activity Reporting
- CA SDM
- CA IAM CS

Contact CA Technologies

Contact CA Support

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

- 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

Providing Feedback About Product Documentation

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

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: Administrative Overview 9

Access the CA Identity Governance Portal 9
User Interface Considerations 9
Language Support 10
Certification 10

Chapter 2: Running a Connector 11

Run or Schedule a Connector Job 11
Verify Mapping of the Login Field 12

Chapter 3: Certifications 13

Certification Overview 13
Use Case: Certify User Privileges Following an Acquisition 14
Use Case: Certifying Privileged Accounts 14
Certification Types 15
Entity Certification 15
Comparative Certification 16
Recurring Certification 16
Start a New Certification 17
Examples: Filter by Attribute 18
How Certifications Apply Pre-approved Violations 19
Create a Certification Template 19
Certification Prerequisites 19
General Information 20
(Recertification/Differential Certifications Only) Filter 20
Reviewers 21
Execution 30
Notifications 30
Email Escalations 31
Certification Properties 31
Recurring Certifications 32
Summary 33
Save Certification Decisions to an Audit Card 34
Import Previous Decisions Into a Certification 35
Usage Information from CA User Activity Reporting in a Certification 35
Share My Work 36

Chapter 4: Business Policy Compliance 37

The Audit Properties File 37
Additional Weighted Attributes 38
Manage Business Policy Rules 39
How to Work with Business Policies 40
Create a Business Policy 40
    Create Business Policy Rules 41
Run a Business Policy Against a Configuration 50
Ignore Specific Violations During Audit Checks 50
    Add Pre-Approved Violations 51
    Configure Pre-Approved Violations 51
    Configure Cleanup Task for Expired Pre-Approved Violations 52
    Enable Web Services for Pre-Approved Violations 52
    Use Case: Pre-Approved Violations 53

Chapter 5: Configure Email Notifications 55

Create an Email Template 56
Select Event Triggers and Assign Templates 57
Define Email Properties 58

Chapter 6: View Changes to Users, Roles, and Resources 61

View the Transaction Log 61
Track Portal Usage in the Transaction Log 62

Chapter 7: Standard Reports 65

Certification 65
Certification by Application 65
Certified Resources with Violations Highlighted 66
Entitlement Quality 66
Policy Information 66
Policy Violation 66
Resources Overview 66
Role Details 66
Roles Overview 67
Users Overview 67
Connect to the Report Server 68
Create a Database Connection to the Report Server 68
Configure Permissions on the Connection Object 69
Extract Data for Reports and Dashboards 70

Create Custom Reports 70

Chapter 8: Business Workflows 73

Administer Business Workflows 74
Filter the Workflow List 75
Monitor Workflow Progress 76
View Workflow Progress by Entities or Reviewers 76
Start and Stop Workflows 77
Define and Send Escalation Emails 77

Chapter 9: How to Perform Data Transformations 79

Introduction 79
Create and Apply Data Transformations 80
How to Define a Universe 85
Import and Verify Data 93

Chapter 10: System Maintenance 95

Repair CA Identity Governance Configuration, User, and Resource Files 95
Purge Data 96
Purge by Document 97
Purge by Date 98
Purge Portal Users from the Permissions Configuration 99
Purge Workpoint Jobs Associated with a Workflow 101

Chapter 11: Troubleshooting 103

Trace Workflow 103
Error Messages 103
Resources Do Not Appear in BPR Drop-down List 112
Using the Pipe Character (|) in Regular Expressions 113
Property: bpr.sod.ignore.zero 113
Property: bpr.all.representative 114
System Checkup 114
SMTP Checkup 115
Workpoint Checkup 115
JMS Queue Checkup 115

Chapter 1: Administrative Overview

This section contains the following topics:

Access the CA Identity Governance Portal (see page 9)
Certification (see page 10)

Access the CA Identity Governance Portal

You can access the web-based CA Identity Governance interface from any system.

Follow these steps:

1. Open a web browser and do *one* of the following:
   - To use a non-SSL connection, enter the following URL:

     `http://ServerName:Port/eurekify`
   - To use an SSL connection, enter the following URL:

     `https://ServerName:HTTPSPort/eurekify`

   The Login screen opens.
2. Enter your credentials.

   Note: The password is case-sensitive.
3. Click Log In.

   The CA Identity Governance Portal Home page appears.

User Interface Considerations

You can use the following usability features available in the screens of the CA Identity Governance Portal:

- Autocomplete: In fields that reference field names or values of a data file, the portal completes your typing with matching values from the data file. You can also press the Down Arrow key to scroll through a list of available field values.
- Mandatory fields: Fields marked with an orange dot are mandatory. You must fill in these fields to proceed to the next stage of a process.
- Customizable Tables: Click Customize in the header bar of a table to change the columns shown and the order in which they are displayed. Click a column header to sort the table by the values of that column. You can also use the Records per page drop-down to limit or extend the size of a long table.

Language Support

The CA Identity Governance Portal appears in the language you selected during installation. To ensure that text, 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 Portal.

Certification

CA Identity Governance uses certification to enable designated reviewers to verify that the relationships, or links, between users, roles, and resources are up-to-date and correct. Certification ensures that granted privileges comply with business and regulatory needs, and that they are not over-allocated. The Audit Card facility supports this process by enabling the reviewer to view out-of-pattern and non-compliant information. An Audit Card contains a list of all suspicious records and the type of suspicion involved.

Chapter 2: Running a Connector

This section contains the following topics:

Run or Schedule a Connector Job (see page 11)
Verify Mapping of the Login Field (see page 12)

Run or Schedule a Connector Job

CA Identity Governance can work with data from various endpoint systems across your organization to analyze user permissions and access to resources, perform role discovery, certifications and more. Connectors enable you to import data from and export data to endpoint systems. Before you run or schedule a connector job, you must define a connector.

Note: For more information about defining a connector, see the *Configuration Guide*.

Follow these steps:

1. In the CA Identity Governance Portal, go to Administration, Universes.
2. Click the universe where you want to run the connector.
3. Click the Connectivity tab.
4. Select Import or Export.
5. Select the check box next to the connectors you want to run.
6. Do *one* of the following:
   - Click Import Now.

     The connector job begins immediately.
   - Click Schedule Selected.

     The Schedule Import Job screen appears. Complete the following fields:
     - First execution—Specifies the date and time when the job first runs.
     - Additional repeats—Defines the number of times you want to run the job. Enter -1 to define an unending series.
     - Repeat interval—Defines the time period between executions in the series.

- Click Schedule All.

  All defined connectors are scheduled according to the values in the Schedule Import Job screen. Complete the following fields:

  - First execution—Specifies the date and time when the job is first run.
  - Additional repeats—Defines the number of times you want to run the job. Enter -1 to define an unending series.
  - Repeat interval—Defines the time period between executions in the series

  Note: Schedule All always runs all connectors in a universe. So, if a connector is added after you schedule all connectors to run, CA Identity Governance includes the new connector in the next scheduled run.

7. Click OK.

   The selected connectors are run or scheduled.

Note: To cancel a scheduled connector job, to go Administration, Job Scheduler and click Delete next to the job you want to cancel.

Verify Mapping of the Login Field

When CA Identity Governance runs an import, it creates new user records based on endpoint data. The product also automatically creates accounts for these users in the CA Identity Governance Portal. To support the Portal login, the import connector job must map a valid value to the login field of the target universe.

Follow these steps:

1. Verify that the target universe has a defined login field:
   a. In the CA Identity Governance Portal, go to Administration, Universes.
   b. Locate the universe you specified for the connector job, and click Edit.
   c. Verify that the Configuration Users Login Field refers to an existing field in the universe. If the Configuration Users Login Field is blank, define it by selecting a field.
   d. Note the name of the Configuration Users Login Field.
2. Verify that the connector maps data to the login field:
   a. Open the mapping XML file you specified for the connector job.
   b. Locate the line that maps the Login field. The line contains the following term:

      ```
      host='Login'
      ```

   c. Verify that endpoint data is mapped to this field in the **guest** term. If this mapping is blank, define it by specifying an endpoint data field.

Chapter 3: Certifications

This section contains the following topics:

Certification Overview (see page 13)
Certification Types (see page 15)
Start a New Certification (see page 17)
Create a Certification Template (see page 19)
Save Certification Decisions to an Audit Card (see page 34)
Import Previous Decisions Into a Certification (see page 35)
Usage Information from CA User Activity Reporting in a Certification (see page 35)
Share My Work (see page 36)

Certification Overview

Certification is the process of verifying that links between users, roles, and resources are true and correct. Certification enables you to review role hierarchy, user privileges, and business rules that you define in CA Identity Governance. When you initiate a certification, CA Identity Governance automatically invites managers to review and certify the access privileges of the users or resources they administer. CA Identity Governance provides tools to customize, track, and manage the certification process, and to implement changes indicated by reviewers.

Certifications support the following business cases:

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

During a certification, a business manager can perform the following actions:

- Review and certify any links directly assigned to them
- Reassign certification items
- Add a comment, file, or link to certification items
- View CA User Activity Reporting information when reviewing certification items

A compliance officer can perform the following actions:

- Monitor certification progress
- Send escalation emails to participating reviewers
- Initiate the approval and implementation phase of the certification

An administrator can perform the following actions:

- Create certification templates
- Save certification decisions to an Audit Card

Use Case: Certify User Privileges Following an Acquisition

New users and resources are added to the model configuration following an acquisition. Administrators run a certification to verify that the privileges assigned to these new users are appropriate.

The stages of the certification are as follows:

1. The role engineer creates a certification that certifies user entitlements. The role engineer defines user attribute filters that limit the scope of the certification to the new employees. A member list maps managers to the new users and resources.
2. Each manager reviews the privileges assigned to their workers. For example, Bob Smith reviews the privileges given to Hector Torres, and suggests access to a database that Hector needs in his new position.
3. CA Identity Governance sends an email to Deepak Chamarti, the owner of the database. Deepak approves the change, and CA Identity Governance updates the configuration file. Hector Torres now can access the database.

Use Case: Certifying Privileged Accounts

You can certify privileged accounts using information that is imported from the CA ControlMinder vault. This certification allows you to govern the access of your users and make sure that they do not have more access than they need.

Follow these steps:

1. Configure the CA ControlMinder connector as follows:
    a. In the Portal, go to Administration, Universes, and select a universe.
    b. Click the Connectivity tab and click Add Connector.

c. Select the CA ControlMinder (Shared Accounts) connector and click Next.

d. Enter the CA ControlMinder Report Database credentials.

Important! The CA ControlMinder connector must be the only connector in the universe.

2. Run the connector to import the privileged account data.

   Note: If the CA ControlMinder Server is unavailable, or to import privileged account information from another source, you can manually create the CSV files using the PUPM.ktr PDI transformation. Then select the CA ControlMinder (Shared Accounts, via CSV) connector and supply the paths to the CSV files you created.

3. Once the user-account information is imported into the product, run an Account Certification as follows:

   a. In the Portal, go to Compliance Management, New Certification.

   b. Under Template, select Account Certification.

   c. Continue with the certification wizard, selecting the appropriate options.

   d. Start the account certification.

Certification Types

Certifications support various business needs. This section details the different types of certifications you can run.

Entity Certification

You can review and certify links between user, role, resource, and account entities in a configuration. You can perform the following entity certifications:

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

  Use this type of certification to document compliance with data security measures.

- Role Certifications—certify the resources, parent or child roles, and users linked to each role. In CA Identity Governance roles are defined as common sets of links. Typically, the owner of each role reviews the links that define their role, and the users who were assigned to the role.

  Use this type of certification to maintain the role hierarchy.

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

  Use this type of certification to monitor access to resources.

- Account Certifications—certify users linked to each account. Typically, a compliance officer reviews users assigned to accounts. You can also use account certification to certify privileged user accounts from CA ControlMinder (PUPM).
- Self-attestation Certifications—a user certification in which each user under review certifies their own privileges.

Comparative Certification

Similar to entity certification, comparative certifications are based on an existing certification. These certifications allow you to create new certification items, and show past decisions on certification items. You can perform the following comparative certifications:

- Recertification—creates a set of certification tasks that are based on a previous certification. Use this type of certification when you require multiple reviews before changes are implemented. For example, you can recertify a self-attestation certification, with managers instead of workers. The managers can see the results of user self-certification as they perform their review.
- Differential Certification—certifies new links added to the configuration that were not included in a previous certification.

Recurring Certification

You can define a series of simple certifications that repeat at regular intervals. Each certification in the series is based on its predecessor.

Note: Every certification must have a unique name and description. When you create a series of recurring certifications, use system variables to give each certification in the series a unique name and description. Typically these fields are based on the certification template. CA Identity Governance replaces system variables with actual text and date values when it creates each certification.

Use the following system variables to create string values for the Name and Description fields:

$sourceCampaignName

Inserts the text string in the Name field of the certification in the series.

$reoccurring

Inserts a number that indicates what iteration the named certification is in the series.

$date

Inserts the date when the certification in the series is created.

$sourceCampaignDescription

Inserts the text string in the Description field of the certification in the series.

Example: Recurring Certification Names

When you create a recurring certification, the Name field of the Basic Information screen is automatically populated with the following formula:

```
$sourceCampaignName Recurring # $reoccurring @ $date
```

If the source certification is named UserCert and the series repeats daily, the first three certifications in the series are named as follows:

```
UserCert Recurring # 1 @ 12Nov2010
UserCert Recurring # 2 @ 13Nov2010
UserCert Recurring # 3 @ 14Nov2010
```

Start a New Certification

As a Compliance Officer, you want to certify that all employees in your organization have the correct entitlements, and that all access granted to your employees complies with specified business policies. To verify compliance, start a new certification that requires all business managers to review and approve or reject all entitlements for a given certification.

Follow these steps:

1. In the Portal, go to Compliance Management, New Certification.
2. Select a template for your certification and provide general information about the certification.
3. Schedule the certification to start immediately or at a specific time.
4. Decide what you want to certify and what violations you want to identify.
5. Select if you want reminder emails to be sent automatically, or if you want to manage them manually.
6. Click Finish.

Examples: Filter by Attribute

When deciding what to certify, you can filter the entitlements included in a certification using attribute values. You can also combine several attribute-based criteria.

Note: Recertification and differential certifications use the filters from the source (base) certification, so no filter options appear when starting those types of certifications.

Example: Roles Pending Approval

To certify roles that have been proposed, but not yet approved, define a rule as follows:

1. In the New Certification wizard, under 'What are you certifying?', click Select Roles.
2. Select the ApprovalStatus field.
3. Set the operator to IS.
4. Add the value 'Pending Approval'.
5. Click Add Rule.

Example: User Certification by Function and Location

To certify the entitlements of sales staff in the Texas region, define a rule as follows:

1. In the New Certification wizard, under 'What are you certifying?', click Select Users.
2. Select the Organization field.
3. Set the operator to IS.
4. Set the value to Sales.
5. Click Add Rule.
6. Select the Location field.
7. Set the operator to IS.
8. Set the value to Texas.

How Certifications Apply Pre-approved Violations

When a list of pre-approved violations has been defined, the list filters violations in all certifications according to a defined Audit Card.

The Audit Card is a source of violations when you create the certification, and of pre-approved violations that are defined. Audit card violations for the certification are processed in the following way:

1. CA Identity Governance identifies entitlements under review that appear in the Audit Card that you specify when you create the certification.

The product filters this group of entitlements, depending on the defined pre-approved violations. If a violation is pre-approved, the alert is unavailable.

Create a Certification Template

Use the certification wizard to create templates for Compliance Officers to select from when running certifications. These templates contain most of the information that is required when starting a certification.

Follow these steps:

1. Review the certification prerequisites.
2. In the Portal, go to Compliance Management, Certification Templates.
3. Select the universe where you want to apply the template.
4. Click Add Template.
5. Move through the steps in the wizard, and provide the appropriate information.
6. Click Finish to save the template.

Certification Prerequisites

Before you define a certification template, do the following:

1. Plan the type (see page 15), scope, and other features of the certification to meet your strategic business needs.
2. Verify that the data used in the certification is updated and accurate, and create additional files needed for the certification. These files can include:
   - Configuration files based on the model configuration of the universe
   - Audit cards that provide violation alerts or suggested links in the certification

- Member lists and RACI configuration files that map reviewers in the certification
- Customized email templates for the various messages that CA Identity Governance sends to certification participants

General Information

Provide general information about the certification template, and select what type of template you want to create. The following fields are not self-explanatory:

Template Type

Specifies the type of certification (see page 15) you create.

Select Configuration

Sets the model as the configuration file for certification or allows a Compliance Officer to select a configuration file when he starts the certification. The product creates the certification based on the roles and links of the selected configuration.

Default: Set the model as the certification configuration file.

(Recertification/Differential Certifications Only) Filter

When you create a recertification or differential certification template, you can define filtering criteria that limit the entities and entitlements included in the certification. These filters alter the nature of the certification to support specific business needs.

States

Specifies which entitlements are included in a recertification or differential certification, based on their last status in the previous certification. You can select the following options:

Pending

Includes entitlements that were not reviewed in the previous certification.

Approved

Includes entitlements that were approved in the previous certification.

Rejected

Includes entitlements that were rejected in the previous certification.

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

Reset Approver's Selection

Omits the decisions of previous reviewers from the current certification.

Show Approver's Selections

Reviewers can override the previous decision.

Update Entitlements

Specifies whether to add entitlements from the configuration that were not in the previous certification. You can select the following options:

Add entitlements that were not included in the source certification

New and excluded entitlements in the configuration are included in this certification.

Do not update

This certification only includes entitlements that were in the previous certification.

Reviewers

Configure the reviewers for each user, role, and resource under review during a certification.

The product can look for reviewers using multiple methods. If no reviewer is identified, the product assigns the review task to a default user.

Using RACI analysis of the model configuration

Selects users based on their relationship to the entity under review.

RACI (Responsible, Accountable, Consulted, Informed) are standardized descriptions for how a user relates to an entity. To find RACI users for each role or resource, the product analyzes privileges and entity attributes in the configuration files of the universe. For example, the user that is listed as the owner of a resource is designated as Responsible for that resource.

(Comparative Certifications Only) You can also select to keep the accountable or accountable manager from the previous certification.

Using this default reviewer

If the product cannot identify reviewers using other methods, specify a default user.

Enable managers to select an entire column

Displays the Select All column for Approve, Reject, and Reassign columns in certification action screens.

How CA Identity Governance Assigns Reviewers

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

In certifications, the product can assign reviewers in the following ways:

- Searches a predefined member list in the server for a user that is related to the entity
- Searches the RACI configuration of the universe for a user who is Accountable or Responsible for the entity

  Note: In user certifications, the product first queries the Configuration Users Manager Field defined in the target universe to identify the manager of each user.
- Assigns the task to a default reviewer defined for the certification
- Let users approve their own links (self-attestation certifications only).

In recertification and differential certifications, the product can assign reviewers in the following ways:

- Searches a predefined member list in the server for a user that is related to the entity.
- Searches the RACI configuration of the universe for one of the following users:
  - A user who is Accountable or Responsible for the entity in the current configuration.
  - The reviewer assigned in the previous certification.
  - The manager of the previous reviewer, based on the Configuration Users Manager Field that is specified for the target universe.
- Assigns the task to a default reviewer defined for the certification

When you create a certification, you can define how the product locates a reviewer, and in what order reviewers are evaluated.

Example: Assign a Reviewer

You can set the product to find reviewers for an entity in the following sequence:

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

Member Lists

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

Each record in a member list contains the following fields:

Login

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

Category

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

Value

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

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

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

You can import member list files into the product or use administrative screens of the portal to create and edit member lists.

Example: Match Reviewers to Resource Attributes

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

Login	Category	Value
DOMAIN\Hector_Torres	ResName3	Solaris
DOMAIN\Anna_Chiu	Location	Atlanta
DOMAIN\Alex_Patrick	ResName3	WinNT
DOMAIN\Kim_Bell	Organization	Marketing Sun Server

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

- The Domain_Users resource with the following attribute values:

  ResName3 = Solaris

  Location = Atlanta

  CA Identity Governance uses the *first* matching record in the list, and assigns Hector Torres to review links for this resource.

- The Purchasing resource with the following attribute values:

  Organization = Headquarters

  No records in the member list match this entity. The product cannot assign a reviewer based on the member list.

More information:

Create a Member List (see page 24)
Create a Member List from a CSV File (see page 25)
Special Characters for Member Lists (see page 26)

Create a Member List

Use a member list to assign reviewers for a certification. Use this procedure to create a member list in the Portal.

Follow these steps:

1. In the Portal, go to Administration, Workflow Settings, Manage Member Lists.
2. Select a universe. The new member list is associated with the universe you select.
3. In the Add Member List area, define a new member list. The following field is not self-explanatory:

   Certification Type

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

   Note: Unless you have the proper permissions in the permissions configuration, you will not see the Add Member List option on the screen.
4. Clear the Use CSV file option.
5. Click Add.

   The Edit member list screen appears.
6. Select a configuration to get field names from and click Add.

7. Use the Add, Edit, and Delete options to compose the member list.
8. Click Save.

   Changes are saved to the member list. The new list appears in the table of member lists.

More information:

Create a Member List from a CSV File (see page 25)
Special Characters for Member Lists (see page 26)

Create a Member List from a CSV File

Use a member list to assign reviewers for a certification. Use this procedure to create a member list based on an imported file of comma-separated values (CSV).

Follow these steps:

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

   ```
   login,category,value
   ```

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

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

   ```
   login,category,value
   DOMAIN\Alex_Patrick,ResName3,WinNT
   DOMAIN\Kim_Bell,Organization,Marketing Sun Server
   ```
2. In the Portal, go to Administration, Workflow Settings, Manage Member Lists.
3. In the Add Member List area, define a new member list. The following field is not self-explanatory:

   Certification Type

   Indicates the type of certification that uses the member list. For example, a member list that contains role attributes works with a role certification.
4. Select the Use CSV file option and browse to the CSV file you prepared.
5. Click Add.

   CA Identity Governance creates a member list based on the CSV file. The new member list appears in the table of member lists.
6. (Optional) Click Edit next to the new member list to verify or modify its contents.

Special Characters for Member Lists

The following system properties define special characters that are used to parse comma-separated values (CSV) files for member lists.

memberlist.csv.reader.separator

Defines the character that separates fields in each line of the file. The comma (,) character is used by default.

memberlist.csv.reader.quotechar

Defines the character that encloses field values that have spaces of other special characters. The double-quote (") character is used by default.

memberlist.csv.reader.escape

Defines the escape sequence that is used in the file. The backslash (\) character is used by default.

Example: Backslash Characters in CSV Input

Often CSV input for a member list contains backslash characters in pathnames, as in the following example:

```
Login, Category, Value
DOMAIN\Hector_Torres, ResName3, Solaris\HTorres
DOMAIN\Alex_Patrick, Location, Atlanta
```

By default, the CSV parser treats the backslash character as an escape character. The resulting member list omits backslashes, as follows:

```
Login, Category, Value
DOMAINHector_Torres, ResName3, SolarisHTorres
DOMAINAlex_Patrick, Location, Atlanta
```

To include the backslash character in field values, edit the memberlist.csv.reader.escape system property to define a different escape character.

Note: Select an escape character that does not appear in your data. Do not use the double quote character as an escape character.

RACI Operations

The RACI model is a tool that is used for identifying roles and responsibilities during an organizational audit, making the audit process easier and smoother. The model describes what should be done and by whom during audits and when corporate changes occur.

RACI is an abbreviation for:

R = Responsible, owner of the problem/project.

A = Accountable, one to whom R is accountable and who must sign off (Approver) on work before it is accepted.

C = Consulted, one whose opinion is sought and who can provide information necessary to help complete the work.

I = Informed, one who must be notified of results (but does not need to be consulted).

One of the main purposes of RACI is to identify entity managers (Approvers). Every model configuration that you want to audit must be run through the RACI generator so that the Approvers are listed correctly.

The RACI utility obtains the data fields that you identified when you defined the Universe as manager fields, and it tags them as the Accountables. The user manager data is extracted from the configuration file 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 certification, as the system does not yet have users that are identified as entity Accountables, and cannot send Approver tasks to the correct entity managers. If you have not run RACI, you either receive an error message, or all the entities are sent to the certification owner for approval.

Create RACI Configuration Files

RACI configurations control the assignment of certification or approval tasks to their respective Accountable person. The product automatically creates the Accountable configuration, based on the Owner or Manager fields of the universe.

Note: Update the user database before you generate RACI configurations for the universe.

Follow these steps:

1. In the Portal, go to Administration, Permissions and RACI, Create RACI.
2. Select a universe from the drop-down list

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 Client Tools. On the File menu, click Review Database. This screen allows you to view and delete the files.

Synchronize RACI

Update the RACI configurations periodically so that they reflect changes made to the universe.

Follow these steps:

1. In the Portal, go to Administration, Permissions and RACI, Synchronize RACI.
2. Select a universe from the drop-down list and click Synchronize RACI.

   The product updates the RACI configuration files of the universe.

Note: When you import new users into a universe, the connector can automatically map them to the RACI configuration files of the universe.

By default, RACI synchronization adds new entity data or deletes entities that no longer exist in the universe. RACI synchronization does not update existing links in the RACI configurations.

The following system properties allow RACI synchronization to update existing links:

raci.sync.override.accountable.roles

Determines whether existing roles are updated in the Accountable configuration. When this property is true, the product updates the Accountable configuration when the accountable user of a role changes. To implement this property for a universe, create a property with the following name:

`universe.property.`*`universe_name`*`.raci.sync.override.accountable.roles`

Note: *universe_name* is the name of the target universe.

raci.sync.override.accountable.resources

Determines whether existing resources are updated in the Accountable configuration. When this property is true, the product updates the Accountable configuration when the accountable user for the resource changes. To implement this property for a universe, create a property with the following name:

`universe.property.universe_name.raci.sync.override.accountable.resources`

Note: *universe_name* is the name of the target universe.

continuousUpdates.shouldSyncRaci

Determines whether to synchronize RACI in each notification from CA Identity Manager. The default value is True. Valid values are:

True

Users can specify if they want CA Identity Manager users included in the RACI configuration.

False

Users can specify if they do not want CA Identity Manager users included in the RACI configuration.

continuousUpdtes.shouldUpdatePermissionsConfiguration

Determines whether to synchronize RACI in each permission notification from CA Identity Manager. The default value is True. Valid values are:

True

Users can specify if they want CA Identity Manager users included in the RACI configuration.

False

Users can specify if they want CA Identity Manager users included in the RACI configuration.

Enable Managers to Select an Entire Column

Administrators can let participants in a certification handle related actions as a group. When group handling is enabled, screens that list certification actions display check boxes in the Approve, Reject, and Reassign column headers. Reviewers select these boxes to apply a decision to all the links in the table.

To enable group handling of related certification actions, select the Enable managers to select an entire column option.

CA Identity Manager Role Owners or Administrators as Approvers for CA Identity Governance Roles

To support CA Identity Manager approvers for roles within CA Identity Governance, the Certify building block should utilize the new source for approvers named IM Dynamic.

If you edit the building block and select the IM Dynamic source for approvers, CA Identity Governance dynamically retrieves the approvers for the role from CA Identity Manager at runtime.

Note: This feature only retrieves approvers for roles originating from an import from CA Identity Manager.

Execution

Specify how suggested changes to a configuration are implemented. When reviewers make decisions that create or delete privileges, the managers of the linked entities can also approve these changes.

Request approval before implementing changes

When new or deleted links result from an initial certification, the product initiates a change approval review before it modifies the configuration file.

As each certifier submits changes

The product initiates a change approval review immediately as each certifier submits their decisions.

Note: This is the default option.

After all certifiers complete their reviews

Change approval reviews are held until all certifiers submit their decisions. The certification owner initiates the change approval review with a manual workflow control action. Approve actions are consolidated, and this simplifies the work of reviewers.

Notifications

CA Identity Governance uses a set of pre-defined templates to send email notifications that are related to the certification. Administrators can create alternative templates for one or more email trigger events in a certification. When you create a certification, you can specify which template to use for each email trigger event of the certification.

Before you can assign alternative templates for your certification, administrators must create the templates.

Specify the email templates to use in the Notifications screen of the certification template wizard. This screen lists email events that are relevant to the type of certification you create.

Follow these steps:

1. Select the Active check box next to an email event to enable email notifications for that event.
2. Select an email template for the event from the Template drop-down list for the event.

Email Escalations

Administrators can configure the certification template to send escalation emails to remind reviewers to complete their items for a certification.

Follow these steps:

1. Click the plus (+) icon to add criteria.
2. Configure the following information for the emails you want to send:
   - Send criteria—percentage of the work that is completed by a specific time relative to the due date
   - Email Template—template to use for the sent email
   - Recipient Type—Accountable, Email Address, or Member List
   - Recipient—dynamic options dependent on the recipient type
3. Add more email definitions if necessary. Click the plus (+) icon. To remove email definitions, click the X icons.

Certification Properties

You can set optional certification behavior. The options displayed depend on the type of certification. By default, the product displays the following standard option areas:

Notifications

The product can automatically export changes that result from the certification to relevant managed endpoints.

Approvals administration

Select the options that are related to the change approval review phase of the certification.

Initial certifier of a suggested link automatically approves addition of the link

Reviewers who approved a suggested link in the initial certification review are automatically assumed to approve the addition of the link to the configuration file.

Initial certifier of an existing link automatically approves changes to the link

Reviewers who rejected an existing link during initial certification review are automatically assumed to approve its deletion from the configuration file.

User changes reviewer selection

Specify reviewer selection criteria for changes to user entities.

The following new options are available when you use RACI analysis to assign a reviewer:

Manager

Assigns the action to the manager of the user who is Responsible for the user, role, or resource.

Manager's Manager

Assigns the action to the manager's manager of the user who is Responsible for the user, role, or resource.

Role changes reviewer selection

Specify reviewer selection criteria for changes to role entities.

Resource changes reviewer selection

Specify reviewer selection criteria for changes to resource entities.

Account changes reviewer selection

Specify review selection criteria for changes to accounts.

Recurring Certifications

To enable recurrence for a certification, select the check box under the Recurring screen of the wizard. This option enables you to set filtering criteria that limit the entitlements included in the recurring certification. These filters modify the recurring certification to support specific business needs.

States

Specifies which entitlements are included in a recertification or differential certification, based on their last status in the previous certification. You can select the following options:

Pending

Includes entitlements that were not reviewed in the previous certification.

Approved

Includes entitlements that were approved in the previous certification.

Rejected

Includes entitlements that were rejected in the previous certification.

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

Reset Approver's Selection

Omits the decisions of previous reviewers from the current certification.

Show Approver's Selections

Reviewers can override the previous decision.

Update Entitlements

Specifies whether to add entitlements from the configuration that were not in the previous certification. You can select the following options:

Add entitlements that were not included in the source certification

New and excluded entitlements in the configuration are included in this certification.

Do not update

This certification only includes entitlements that were in the previous certification.

Summary

Review the details of the certification template and click Finish to save the template.

Customize Display of Certifications

You can customize the table layout that is used to display certifications.

Mandatory columns cannot be removed from table displays. Red text and a locked padlock icon indicate mandatory columns in customization screens and dialogs. Some mandatory columns are hard-coded defaults in CA Identity Governance. Administrators can define and position additional mandatory columns.

Follow these steps:

1. In the Summary screen of the wizard, open the Display Settings header.

   This section contains five table headers. The General Actions, User Actions, Role Actions, Resources Actions, and Account Actions headers show the table layouts used to display items in the detail screens.

2. Customize the table layout as follows:

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

   b. Use the arrow icons to add, remove and order the columns.

c. When you finish customizing the columns, click OK to close the Customize window.

d. In the Workflow Display Settings window, click the lock icon next to the column name to make the column mandatory. Users can move a mandatory column, but they cannot remove it.

3. Click OK.

   CA Identity Governance displays items for this certification in the table formats you specified.

Save Certification Decisions to an Audit Card

You can save the decisions that reviewers make in a certification to a data file. This data can form the basis for additional certifications, analytical processes, or manual resolution in endpoint systems.

The data file is a variation of the standard Audit Card format. This Audit Card records the results of the initial certification review. All certification decisions are saved, even if resource owners or managers did not allow the requested changes.

Follow these steps:

1. In the Portal, go to Administration, Workflow Settings.
2. Click Export Certification Progress to Audit Card.

   Note: To export from a campaign that was created in release 3.2, click Export v3.2 Certification to Audit Card.

   The Export Certification Progress to Audit Card screen appears.

3. Select an active certification, and enter the name of the Audit Card that contains saved data.

   Note: If you specify an existing Audit Card, its data is overwritten.

4. Click Export.

   An Audit Card is created with a record of the decisions from the certification that you specified.

Import Previous Decisions Into a Certification

As an administrator, you may want import decisions from an earlier campaign (certification) before the r12.5 SP3 release. You can import the decisions that certifiers made in a previous campaign into a new certification.

Note: You need an Audit Card that contains the exported decisions from the previous campaign to complete this procedure.

Follow these steps:

1. In the Portal, go to Certification Management, New Certification.

   The Certification wizard appears.

2. Create a "placeholder" certification with a Manual Start time.

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

3. Navigate to Administration, Workflow Settings.

4. Click Import Certification Progress from Audit Card.

   The Import Certification Progress from Audit Card screen appears.

5. Specify the placeholder certification and the Audit Card that contains the saved data.

6. Click Import.

   The previous decision information is imported and the certification is archived.

7. Return to Certification Management, New Certification.

8. Create a certification (using the recertification template) that is based on the placeholder certification with the Audit Card decision information in it, and run the certification.

Usage Information from CA User Activity Reporting in a Certification

When CA User Activity Reporting is deployed in your environment, CA Identity Governance can display usage information drawn from CA User Activity Reporting. Reviewers can use this information when they certify links.

When you mouse over an entity, all usage data appears for the entity under review.

You enable and configure data polling between CA Identity Governance and CA User Activity Reporting separately for each universe. When you enable polling of CA User Activity Reporting for a universe, all certifications that are based on that universe display usage information.

Note: For more information about CA User Activity Reporting integration, see the *Configuration Guide*.

Share My Work

As a business user, you may want to share your work with another user for periods when you are out of the office or otherwise unavailable. You can authorize another user to approve or reject certifications on your behalf. Any new certifications that are assigned to you are also sent to the user that you selected. An email is also sent to the selected user, notifying them that there is a certification that they can act on.

The first action that is taken, either by you or the user you are sharing your work with, is then processed by the product.

To select a user to share your work with, click Share my Work in the top right corner of the screen.

Note: This functionality is different from reassigning a certification. When you share your work, the certifications are not reassigned to the user you a sharing with. Instead, the certifications remain assigned to you, even though the other user can act on those certifications.

shareMyWork.enable

Enables or disables the Share my Work option in the Portal.

Default: True

Chapter 4: Business Policy Compliance

This section discusses how to create and work with Business Policy Rules (BPRs).

This section contains the following topics:

The Audit Properties File (see page 37)
Additional Weighted Attributes (see page 38)
Manage Business Policy Rules (see page 39)
How to Work with Business Policies (see page 40)
Create a Business Policy (see page 40)
Run a Business Policy Against a Configuration (see page 50)
Ignore Specific Violations During Audit Checks (see page 50)

The Audit Properties File

CA Identity Governance identifies and lists suspicious users, roles and resources in six categories: suspect entities, suspect connections, similar roles and role hierarchy, similar resources, in/out of pattern entities and entities with many/few connections.

Parameters that specify the criteria for generating these lists are in the audit properties file (default.propertiers.xml) under the following location:

CA_RCM_install\rcm-websphere\rcm-conf\audit\parameters\

If you want to change this file for a specific universe, go to the Client Tools and use the Audit Menu.

Note: For more information about the Audit Menu and editing audit properties, see the *Client Tools Guide*.

Additional Weighted Attributes

CA Identity Governance user and resource entities can have an unlimited number of attribute fields. Any of these attribute fields may be used as statistical weighting factors for an audit process.

The default CA Identity Governance audit properties file (default-properties.xml) provides placeholders for 12 attributes and their corresponding weight values. When you import a configuration file that has more than 12 attributes, define the additional attributes in the audit properties file.

Follow these steps:

1. Determine the number of attributes in the configuration file that you imported.
2. In the CA Identity Governance Portal, click Administration, Settings, Audit Property Settings.
3. Click Browse. Navigate to the following folder of the system on which you ran the CA Identity Governance installer:
   - For JBoss/Windows implementation:

     `gm_install\rcm-websphere\rcm-conf\audit\parameters\`
   - For AIX/WebSphere implementation:

     `gm_install\Server\eurekify-jboss\rcm-conf\audit\parameters\`

   Note: *gm_install* is the CA Identity Governance installation directory.
4. Copy the default-parameters.properties file and rename the copy.
5. Select the copy and click Open.

   The file is saved to the CA Identity Governance database. The file appears in the list of audit properties files.
6. Click the Edit icon for the audit properties file you created.

   Placeholder properties for weighting attributes have the following format:

   `evaluation.weight.field.n`

   Note: *n* is a number from 1 through 12.
7. Add more placeholder properties to match the number of attributes in the configuration file that you imported. Use the same naming convention, and increase the value of *n* in each property name.
8. Click Done.

   Changes are saved to the properties file.
9. Go to Administration, Universes.

10. Click on the target universe for the imported configuration.
11. In the Audit Settings File field, specify the audit properties file that you modified and click Save.

    The target universe uses the audit properties file with additional weighting factors.

Manage Business Policy Rules

A Business Policy Rule (BPR) expresses business, provisioning, or security constraints as a logical condition that can be applied to the entities and links in a CA Identity Governance configuration. For example:

```
<Purchasing> forbidden to be <Subcontractor Payments>
```

You can apply this rule to a CA Identity Governance configuration to ensure that workers who have privileges to order stock from subcontractors do not have privileges to authorize payments to those subcontractors.

Typically a BPR is defined by specifying the following information:

- The type of rule—CA Identity Governance provides a broad range of rules that let you examine and compare various entity values. The rule type that is used in the previous example is Restrict access of users to roles by role access. This type of rule restricts the roles that a user can have based on other roles they already have.
- The logical condition—in our example, users with certain roles are forbidden from having other roles. You can also use this type of rule to allow or require users with certain roles to have other roles.
- Data sets and limit values—in our example, we specify a set of roles that are related to purchasing functions, and another set of roles that grant payment privileges.

A Business Policy is a set of BPRs. This policy (saved as a BPR file) exists independently of any specific configuration. The rules that comprise the policy can be adapted and applied to any CA Identity Governance configuration to verify its logic, integrity, and compliance with policy.

How to Work with Business Policies

Follow these general procedures when you work with BPRs.

To access BPRs, go to Compliance Management, BPR Management in the Portal. The BPR table appears and lists all business policy files in the database.

From this screen, you can perform the following actions:

- To create a business policy, click Add New.
- To edit an existing business policy, click the Edit icon for the policy you want to edit.
- To run an existing business policy on a configuration, click Run.
- To remove a business policy rule from the database, click the Delete icon for the policy you want to remove.

Create a Business Policy

Create a business policy to apply a set of BPRs to a CA Identity Governance configuration.

Follow these steps:

1. In the Portal, go to Compliance Management, BPR Management.

   The BPR list screen appears. The table lists all business policy rules in the database.

   Click Add New.

   The Create BPR screen appears.

2. Specify the settings for the policy. The following field is not self-explanatory:

   Reference Configuration

   The configuration used to create and test the policy.

   Note: Business policies are independent of configuration files. The reference configuration is only used to create and test the policy. You can apply the finished business policy to any configuration.

3. Specify optional behaviors for the policy under Policy Attributes. Options include the following:

   Read Only

   Specifies whether you can edit the policy.

   Logged

   Specifies whether changes to the policy are recorded in the transaction log.

   Completed

   This field is not currently used.

4. Click Save.

   The business policy is created in the database.

   The Edit BPR screen appears.

5. Click Add Rule to create a rule (see page 41).

6. Click Test to test the rule set against the reference configuration.

   You have created a business policy to apply a set of BPRs to a CA Identity Governance configuration.

Create Business Policy Rules

Step through the wizard to create a rule, as follows:

1. Under Basic Information, provide information that describes the scope and purpose of the rule. The following fields are not self-explanatory:

   Score

   A numeric value (0-100) that defines the risk level of a violation of this rule. This score is compared to the universe risk thresholds during certification, and used to categorize warnings for the violation as high, medium, or low.

   Note: For more information about risk thresholds, see the Configuration Guide.

   Default: 50

   Owner

   Defines the user responsible for the rule.

Compliance Message

Defines the message that is displayed when viewing the warning for the rule violation.

Business Area/Business Process

Text fields that define the scope and purpose of the rule. These fields are descriptive and do not affect processing of the rule.

2. Under logic, specify values for the following fields to define the underlying logic of the rule:

   Type

   Specifies the rule type (see page 42) that defines what entities are examined to identify violations.

   Restriction

   Specifies the restrictions (see page 45) for examined entities.

3. Under Data, define the entities that are examined. You can select individual entities, or specify attribute values to select a group of entities.

   Many types of rules compare two sets of entities. In these cases, the Data screen is divided into two areas, left and right, and the logic of the rule is stated in terms of these two groups.

   For other types of rules you define numerical thresholds, date ranges, or text matching patterns.

4. The Summary screen displays rule settings, and lets you test the rule against the reference configuration before you create the rule.

Rule Types

When you create a business policy rule, specify the type of rule you want to create in the Type field of the rule creation wizard.

Together, the rule type and the restriction type define the rule logic.

The following types of rule are available:

Resource – Resource (by Roles)

Roles that include specified resources solely/must/must not/may/can only include specified resources.

This rule corresponds to the resource.resource.byRole rule type in the Client Tools.

Resource – Resource (by Users)

Users that can access specified resources solely/must/must not/may/can only access other specified resources.

This rule corresponds to the resource.resource.byUser rule type in the Client Tools.

Role – Resource (by Roles)

Roles that include specified roles solely/must/must not/may/can only include specified resources.

This rule corresponds to the resource.role.byRole rule type in the Client Tools.

Role – Resource (by Users)

Users that can access specified roles solely/must/must not/may/can only access specified resources. For example, users with the Research or IT role must have access to the Unix Admin resource.

This rule corresponds to the resource.role.byUser rule type in the Client Tools.

Role – Role (by Roles)

Roles that include specified roles solely/must/must not/may/can only include other specified roles. For example, roles that include the Purchasing role cannot include the Finance role.

This rule corresponds to the role.role.byRole rule type in the Client Tools.

Role – Role (by Users)

Users that can access specified roles solely/must/must not/may/can only access other specified roles. For example, only users with the Manager or Sys Admin roles can have the Database Creator or Database Editor roles.

This rule corresponds to the role.role.byUser rule type in the Client Tools.

Segregation of Duty Resources

Use this rule to segregate duties. You specify a set of resources and a target amount of resources. Each user must have more than/exactly/less than the specified number of resources from the specified set of resources.

This rule corresponds to the segregation.role rule type in the Client Tools.

Segregation of Duty Roles

Use this rule to segregate duties. You specify a set of roles and a target number of roles. Each user must have more than/exactly/less than the specified number of roles from the specified set of roles. For example: define a set that includes all roles that let users approve purchases. You can then restrict the number of these roles that users can have simultaneously.

This rule corresponds to the segregation.role rule type in the Client Tools.

User Attribute - Resource

Users with specified attribute values solely/must/must not/may/can only access specified resources.

This rule corresponds to the user.attribute.resource rule type in the Client Tools.

User Attribute - Role

Users with specified attribute values solely/must/must not/may/can only access specified roles. For example, the Marketing_Paris role can only be given to users with the Location attribute equal to France and the Organization attribute equal to Sales.

This rule corresponds to the user.attribute.role rule type in the Client Tools.

User Attribute - Role Attribute

Users with specified attribute values solely/must/must not/may/can only access roles with specified attribute values. For example, only users with the Company attribute equal to Temporary are assigned all roles with the organization attribute equal to Subcontractors.

This rule corresponds to the user.attribute.role.attribute rule type in the Client Tools.

User Attribute Value

Use this rule to select user attribute values. You can define a range of test restrictions on attribute values that check for null values, numerical and date ranges, and text patterns.

This rule corresponds to the user.attribute.value rule type in the Client Tools.

User Counter of Resources

The number of users with the specified resources must be more than/less than/exactly/unequal to the specified numerical limit. When you specify the *forbidden value* restriction, the rule limits the number of users that may *not* have the specified resources - all other users *must* have these resources.

This rule corresponds to the user.count.resource rule type in the Client Tools.

User Counter of Roles

The number of users with the specified roles must be more than/less than/exactly/unequal to the specified numerical limit. When you specify the *forbidden value* restriction, the rule limits the number of users that may *not* have the specified roles - all other users *must* have these resources.

This rule corresponds to the user.count.role rule type in the Client Tools.

Rule Restrictions

Most rules describe a relationship between two groups of entities. You specify the members of these groups when you create a rule. These groups are identified as Left and Right in BPR editing screens. The following table lists the rule types and the restrictions available for each rule type.

Role – Role (by Users)

Only <L> May Have <R>

Only users that have roles on the left may have roles on the right side.

<L> Must Have <R>

Users that have roles on the left must have roles on the right.

<L> Forbidden to Have <R>

Users that have roles on the left must not have roles on the right.

<L> Only Allowed to Have <R>

Users that have roles on the left can only have roles on the right, and no others.

Role – Role (by Roles)

Only <L> May Have <R>

Only roles that have child roles on the left may have roles on the right as children

<L> Must Have <R>

Roles that have child roles on the left must have roles on the right as children.

<L> Forbidden to Have <R>

Roles that have child roles on the left must not have roles on the right as children.

<L> Only Allowed to Have <R>

Roles that have child roles on the left can only have roles on the right as children, and no others.

Role – Resource (by Users)

Only <L> May Have <R>

Only users that have roles on the left may access resources on the right.

<L> Must Have <R>

Users that have roles on the left must access resources on the right.

<L> Forbidden to Have <R>

Users that have roles on the left are must not access resources on the right.

<L> Only Allowed to Have <R>

Users that have roles on the left can only access resources on the right, and no others.

Role – Resource (by Roles)

Only <L> May Have <R>

Only roles that are parents of roles on the left may access resources on the right.

<L> Must Have <R>

Roles that are parents of roles on the left must access resources on the right.

<L> Forbidden to Have <R>

Roles that are parents of roles on the left must not access resources on the right.

<L> Only Allowed to Have <R>

Roles that are parents of roles on the left can access only resources on the right, and no others.

Resource – Resource (by Users)

Only <L> May Have <R>

Only users that can access resources on the left may access resources on the right.

<L> Must Have <R>

Users that can access resources on the left must access resources on the right.

<L> Forbidden to Have <R>

Users that can access resources on the left must not access resources on the right.

<L> Only Allowed to Have <R>

Users that can access resources on the left can access only resources on the right, and no others.

Resource – Resource (by Roles)

Only <L> May have <R>

Only roles that include resources on the left may include resources on the right.

<L> Must have <R>

Roles that include resources on the left must include resources on the right.

<L> Forbidden to have <R>

Roles that include resources on the left must not include resources on the right.

<L> Only allowed to have <R>

Roles that include resources on the left can include only resources on the right, and no others.

User Attribute - Role

Only <L> May have <R>

Only users with user attributes on the left may have roles on the right.

<L> Must have <R>

Users with user attributes on the left must have roles on the right.

<L> Forbidden to have <R>

Users with user attributes on the left are forbidden to have roles on the right.

<L> Only allowed to have <R>

Users with user attributes on the left can have only roles on the right, and no others.

User Attribute - Role Attribute

Only <L> May have <R>

Only users with attributes on the left may have roles with attributes on the right.

<L> Must have <R>

Users with attributes on the left must have roles with attributes on the right.

<L> Forbidden to have <R>

Users with attributes on the left are forbidden to have roles with attributes on the right.

<L> Only allowed to have <R>

Users with attributes on the left can have only roles with attributes on the right, and no others.

User Attribute - Resource

Only <L> May have <R>

Only users with user attributes on the left may access resources on the right.

<L> Must have <R>

Users with user attributes on the left must access resources on the right.

<L> Forbidden to have <R>

Users with user attributes on the left are forbidden to access resources on the right.

<L> Only allowed to have <R>

Users with attributes on the left can access only resources on the right, and no others.

Segregation of Duty Roles

Should have no more than <R> of <L>

Users should have no more than *number* (on right) of the roles on the left.

Should have at least <R> of <L>

Users should have at least *number* (on right) of the roles on the left.

Should have exactly <R> of <L>

Users must have exactly *number* (on right) of the roles on the left.

Segregation of Duty Resources

Should have no more than <R> of <L>

Users should have no more than *number* (on right) of the resources on the left.

Should have at least <R> of <L>

Users should have at least *number* (on right) of the resources on the left.

Should have exactly <R> of <L>

Users must have exactly *number* (on right) of the resources on the left.

User Counter of Roles

Should have no more than <R> Users

Roles on the left should have no more than *number* (on right) users.

Should have at least <R> Users

Roles on the left should have at least *number* (on right) users.

Should have exactly <R> Users

Roles on the left must have exactly *number* (on right) users.

User Counter of Resources

Should have no more than <R> Users

Resources on the left should have no more than *number* (on right) users.

Should have at least <R> Users

Resources on the left should have at least *number* (on right) users.

Should have exactly <R> Users

Resources on the left must have exactly *number* (on right) users.

User Attribute Value

Number <L> must be greater than <R>

The numeric value of the user attribute on the left must have a greater value than the numeric value on the right.

Number <L> must be less than <R>

The numeric value of the user attribute on the left must be less than the numeric value on the right.

Number <L> must be equal to <R>

The numeric value of the user attribute on the left must be equal to the numeric value on the right.

Date <L> must be earlier than <R>

The date for the user attribute on the left must be earlier than the date on the right.

Date <L> must be later than <R>

The date for the user attribute on the left must be later than the date listed on the right.

<L> Must match regular expression <R>

The value for the user attribute on the left must match the value defined by the regular expression on the right.

<L> Must not match regular expression <R>

The value for the user attribute on the left must not match the value defined by the regular expression on the right.

<L> Should be empty

The value for the user attribute on the left should be empty.

<L> Should not be empty

The value for the user attribute selected on the left should not be empty.

Run a Business Policy Against a Configuration

When you apply a business policy to a configuration, CA Identity Governance analyzes the configuration to find entities and links that violate the rules of the policy. The result is an Audit Card that contains all violations of policy that were found in the configuration.

Follow these steps:

1. In the Portal, go to Compliance Management, BPR Management.

   The table lists all business policies in the database.

2. Click Run.

3. Specify values for the following fields:

   Audit Card

   Defines the name of the Audit Card that contains any violations that are found in the target configuration.

   Configuration

   Specifies a configuration file in the database that is the target for business policy analysis.

4. In the Select BPRs area of the screen, select the business policy that you want to apply to the target configuration.

5. Click Run.

   The Audit Card is created, and analysis of the configuration begins. If no violations are found, the empty Audit Card is deleted from the database.

Ignore Specific Violations During Audit Checks

To gray out or ignore (hide) specific violations when performing compliance and pattern checks, you can add pre-approved violations within a specific universe. Pre-approved violations appear on certification and self-service violation screens.

When adding pre-approved violations, you can provide an expiration date. Once the date expires, the violation is no longer pre-approved and behaves as a regular violation once again. You can also provide a comment to explain the reason to approve the violation.

If a pre-approved violation has an expiration date or an explanation provided, both appear in the violation tooltip when you mouseover the violation.

A scheduled task runs at a configurable interval, searches through all universes that have an approved Audit Card, and deletes all expired alerts.

Add Pre-Approved Violations

For each universe, you can set violations as pre-approved. These pre-approved violations are ignored (hidden) or unavailable in compliance and pattern check Audit Cards.

Note: **You need administrator-level rights in the Portal to perform this procedure.**

Follow these steps:

1. In the Client Tools, connect to the CA Identity Governance server.
2. Open the Audit Card that contains violations that you want to pre-approve.

   Note: A violation must be saved to the database before you set it as pre-approved.
3. (Optional) Provide an expiration date or a comment:
   a. Right-click the violation and select Edit.
   b. To set an expiration date, select the Expiration Date option and provide a date.
   c. To provide a reason for the pre-approval, go to the Pre-Approve comment field and enter text.
   d. Click OK.
4. Right-click the violation that you want to pre-approve and select Always Approve this Violation.

   Note: The Client Tools must connect to the CA Identity Governance Portal rather than the Microsoft SQL Server directly to see this option.
5. Verify that the violation appears in the Audit Card titled *universe_name* Pre-Approved Violations.

Configure Pre-Approved Violations

If you added pre-approved violations to a universe, you can specify whether the violation is dimmed or is ignored (hidden) altogether. You configure pre-approved violations under Universes.

To configure pre-approved violations

1. In the CA Identity Governance Portal, go to Administration, Universes.
2. Locate the universe with the pre-approved violations to configure, and click Edit.
3. Next to 'Approved alerts are:', select the display configuration you want for pre-approved violations.

   Default: Dimmed
4. Click Save.

Configure Cleanup Task for Expired Pre-Approved Violations

In CA Identity Governance, you can enable or disable a scheduled task to search through all universes that have an approved Audit Card, and delete all expired alerts. This scheduled task can be configured using the CA Identity Governance portal.

Follow these steps:

1. In the CA Identity Governance portal, go to Administration, Settings.
2. Click Property Settings.
3. Click Edit and change either of the following settings:
   - audit.delete.expired.alerts.enabled—enables or disables the cleanup of expired pre-approved violations

     Default: True (enabled)
   - audit.delete.expired.alerts.interval.seconds—second interval between each cleanup

     Default: 86400 (one day)

   Note: To override the default behavior for a specific universe, create a universe-specific property, for example, you can create the property universe.property.*Universe* \ *Name*.audit.delete.expired.alerts.enabled and set it appropriately for that universe. Spaces in a universe name are replaced with a backslash followed by a space (\ ).
4. Click Save.

Enable Web Services for Pre-Approved Violations

By default, web services do not include pre-approved violations. To include pre-approved violations, set the following property:

```
audit.approved.alerts.webservices.include=true
```

If you want to override the default behavior for a specific universe, create a universe-specific property and set it to true:

```
universe.property.My\ Universe\
Name.audit.approved.alerts.webservices.include=true
```

Note: Spaces in a universe name are replaced with a backslash followed by a space (\ ).

Use Case: Pre-Approved Violations

You need a few people from the Human Resources department to help the Finance department during a busy time at the end of the year.

The employees from the Human Resources department must access financial resources that would typically generate a violation within CA Identity Governance.

First, grant the Human Resources employees access to the financial resources, then test for compliance, and add the resulting violations to the pre-approved violations list. Finally, set the expiration date of each pre-approved violation to the first day of the next year.

Note: Remember to enable the scheduled job that deletes expired pre-approved violations.

All violations that are generated by this temporary work situation are suppressed until the end of the year. Depending on universe settings, these violations are hidden or dimmed in certification screens or self-service validation screens based on the universe.

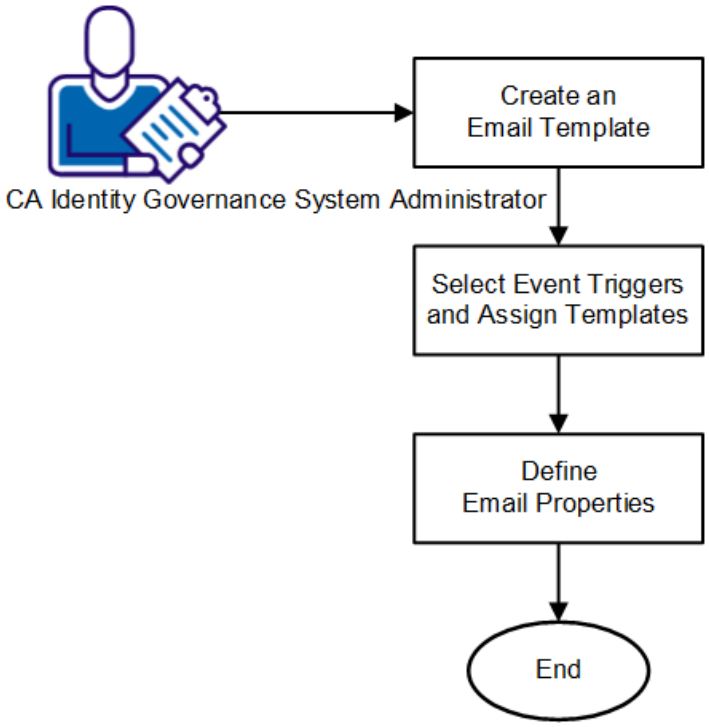
Chapter 5: Configure Email Notifications

The CA Identity Governance server dispatches email notifications at various certification stages, and for self-service requests. The emails use a set of templates that are stored in the server.

You can customize email behavior by creating different templates, and disabling emails for certain events.

For example, you can create one set of email templates for user privileges certification by direct managers and another set for recertification by higher-level managers. You select the email templates to use when you create each certification.

The following diagram illustrates how to configure CA Identity Governance email notifications:



Follow these steps to configure CA Identity Governance certification email templates:

1. Create an email template (see page 56).
2. Select event triggers and assign templates (see page 57).
3. Define email properties (see page 58).

Create an Email Template

Use parameter fields to insert personalized data in CA Identity Governance email templates.

You can base a CA Identity Governance email template on an existing template or create a new template, and use parameter fields to personalize your template.

We recommend that you base your first customized template for an email trigger event on the default CA Identity Governance template that is defined for that event.

Note: You cannot edit or delete a built-in template.

Follow these steps:

1. In the CA Identity Governance Portal, go to Administration, Settings, Email, Templates.

   The Email Templates screen appears.

2. To create an email template, do **one** of the following:

   - Base the new template on a built-in template:

     a. Click Load.

        The Load Template dialog appears.

     b. Select a template for the trigger event from the Select drop-down list and click OK.

        The template appears in an editing screen.

     c. Click Save As and rename the template.

   - Create a template:

     a. Click New.

        The New Template dialog appears.

     b. Select the trigger event that uses this template from the Email Event drop-down list.

     c. Specify a template name in the Name field.

     d. Click OK.

     The Email Templates editing screen appears.

3. Edit the template text.

4. (Optional) To add a parameter field, do the following:
   a. In the Subject or Body areas of the template, position your cursor where you want to insert the field.
   b. Locate the parameter in the Parameters list table below the template editing window.
   c. Click Add to Subject or Add to Body next to the field in the table.

   The parameter is inserted into the template. When emails are sent, actual data replaces the selected parameter.
5. (Optional) To insert HTML elements in the email template, do the following:
   a. In the Subject or Body areas of the template, position your cursor where you want to insert HTML.
   b. Add the HTML text.
6. Click Save to save the template.

   You have created a custom email template.

Next, you specify certification events.

Select Event Triggers and Assign Templates

Specify certification events to generate CA Identity Governance certification emails.

Follow these steps:

1. In the CA Identity Governance Portal, go to Administration, Settings, Email, Events.

   The Email Events window displays a list of events that trigger emails.

   Note: This screen displays legacy events and templates from previous versions of CA Identity Governance. Legacy events are listed at the bottom of the table, and have separate Aggregation Templates. Do not activate these events.
2. Select the events that you want to trigger emails, and clear events that you do not want to trigger emails.
3. (Optional) Select an alternative template for the event in the Template drop-down list of the event.
4. Click Save to save settings.

   The selected events are enabled and templates assigned.

   Next, you define CA Identity Governance certification email properties.

Define Email Properties

Define CA Identity Governance email properties to customize email notifications.

Follow these steps:

1. In the Portal, go to Administration, Settings, Property Settings.

   The list of properties appears.

2. Use the following system properties to configure the connection to an SMTP server, and to define email behavior.

   Note: Some of these properties are automatically set during CA Identity Governance installation.

   mail.Server

   Defines the SMTP server URL.

   Default: smtp.company.com

   mail.ServerPort

   Defines the communication port for the SMTP server.

   Default: 25

   mail.user

   Defines the CA Identity Governance user account on the SMTP server.

   Default: DemoV4@Eurekify.com

   mail.password

   Defines the CA Identity Governance account password on the SMTP server.

   Default: abc1234

   mail.from

   Defines the CA Identity Governance server originating email address.

   Default: RCM@ca.com

   mail.useSSL

   Specifies whether SMTP server communication uses SSL encryption.

   Default: False

   (Optional) mail.max.attempts

   Defines the number of times CA Identity Governance attempts to send an email.

   Default: 3

(Optional) mail.sending.interval

Specifies the time, in seconds, between CA Identity Governance attempts to send emails.

Default: 900 seconds

(Optional) mail.smtp.timeout

Specifies in seconds, CA Identity Governance email timeout attempts to send emails.

Default: 60 seconds

portalExternalLink.certificationUrl

Defines the value of the certification URL parameter in email templates.

portalExternalLink.homeUrl

Defines the value of the CA Identity Governance URL home page parameter in email templates.

3. Click Save.

You have defined the email properties.

Chapter 6: View Changes to Users, Roles, and Resources

This section contains the following topics:

View the Transaction Log (see page 61)
Track Portal Usage in the Transaction Log (see page 62)

View the Transaction Log

The CA Identity Governance Transaction Log (TxLog) provides detailed information about actions taken in the CA Identity Governance server. The transaction log also records all changes to user, role, and resource entities.

A table summarizing transaction log entries is located in the Developer Resource directory of the **CA-RCM-***rel#***-Language-Files.zip** file of the CA Identity Governance installation package.

When you first open the Transaction Log page, the table is empty and you can view a filter that you can use to select which transactions you want to view.

Note: To register changes made through the Client Tools in the transaction log, configure the Client Tools to work in Connected Mode, and save the configuration with the 'Use modification service' check box enabled.

To view transactions in the Transaction Log table

1. In the CA Identity Governance Portal, go to Administration, Transaction Log.

   The Transaction Log screen opens.

2. (Optional) Filter the data you want to view in the Transaction Log table by filling out the following two fields:

   <Column>

   Select the object that determines which transactions are viewed in the Transaction Log table. You can filter on the following options:

   - Source: The subsystem where the transaction originates
   - 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.

3. Click OK.

   The requested transaction logs appear in the Transaction Log table.

4. (Optional) Click Delete All to delete all the transactions currently saved by the system.

Track Portal Usage in the Transaction Log

The CA Identity Governance server records user actions and changes to entities in its transaction log file. You can track user interaction with the CA Identity Governance Portal in the transaction log.

Note: **You need administrator-level rights in the Portal to perform this procedure.To track Portal usage in the transaction log**

1. In the CA Identity Governance Portal, go to Administration, Settings, Property Settings.

   The Properties Settings window appears.

2. Modify the following CA Identity Governance 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 Identity Governance 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 Identity Governance 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 Identity Governance Portal.

   Values: True, False

txlog.portal.pageaccess.enable

Specifies whether to record events in the transaction log when users navigate in the CA Identity Governance Portal.

Values: True, False

txlog.portal.pageaccess.include.pageclasses

Specifies the pages of the portal to include when tracking user navigation in the CA Identity Governance portal. Identify pages of the portal by their class names, and format the list as comma-separated values.

Example: The following string enables tracking of user navigation to the portal homepage and the top-level dashboard and entity browser pages:

```
com.eurekify.web.portal.homepage.HomePage,com.eurekify.web.dashboards.ConfigurationDashboardPage,com.eurekify.web.entitybrowser.EurekifyBrowserPage
```

txlog.portal.pageaccess.exclude.pageclasses

Specifies the pages of the portal to exclude when tracking user the navigation in the CA Identity Governance 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 Identity Governance Portal are recorded in the transaction log as defined.

Chapter 7: Standard Reports

Out of the box, CA Identity Governance reporting service comes with standard reports that are deployed as part of the report portal installation.

Note: The report title is the name as it appears in BusinessObjects InfoView.

The following list is the list of reports available:

- Certification (see page 65)
- Certification by Application (see page 65)
- Certified Resources with Violations Highlighted (see page 66)
- Entitlement Quality (see page 66)
- Policy Information (see page 66)
- Policy Violation (see page 66)
- Resources Overview (see page 66)
- Role Details (see page 66)
- Role Overview (see page 67)
- Users Overview (see page 67)

Certification

The CA Identity Governance Certification report displays a list of all the associated users and entitlements.

The Certification report lists according to certifier and the entity that is being certified.

Certification by Application

The CA Identity Governance Certification by Application report displays a list of all the users and roles that are associated with each application in your system.

The Certification by Application report lists according to application entitlements.

Note: This CA Identity Governance report is used for a configuration that is obtained by a CA Identity Manager connector that has an application field mapped in the universe.

Certified Resources with Violations Highlighted

The CA Identity Governance Certified Resources with Violations Highlighted report displays a list of certified resources with highlighted violations. You can export the report to Microsoft Excel format to filter violations and information. The report appears in all languages specified by your localization settings.

Entitlement Quality

The CA Identity Governance Entitlement Quality report displays a list of entitlements that are assigned directly to the user, and entitlements that are indirectly granted to the user by a role.

The Entitlement Quality report lists according to the user.

Policy Information

The CA Identity Governance Policy Information report displays a list of compliance policy rules.

The Policy Information report groups policy rules by risk level.

Policy Violation

The CA Identity Governance Policy Violation report displays a list of all compliance policy rules and those users who violate the rules.

Resources Overview

The CA Identity Governance Resources Overview report displays a list of resources based on the selected filter.

Role Details

The CA Identity Governance Role Details report displays the lists of relating users, resources, and sub roles for a given role.

Roles Overview

The CA Identity Governance Roles Overview report displays key statistics on the Role Model. After these statistics are the counts of users, resources, sub roles and of relating policy violations, for each role.

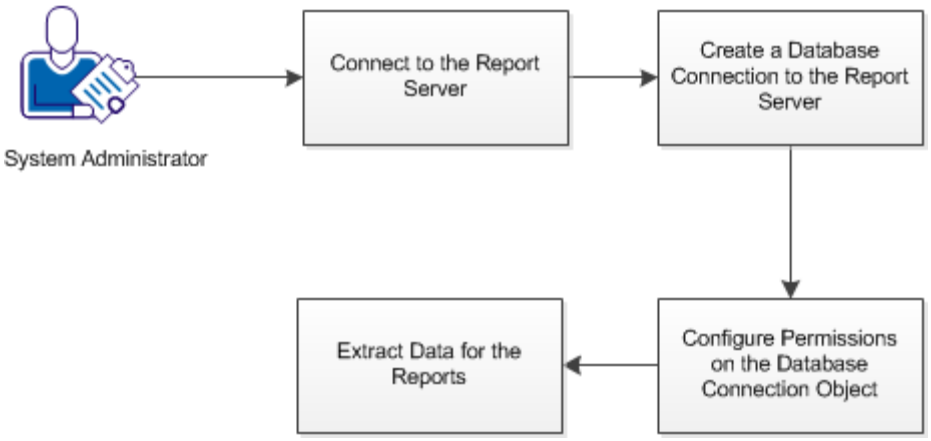
Users Overview

The CA Identity Governance Users Overview report displays a list of resources that are based on the selected Organization Type and Organization Name.

How to Configure Reporting

As an administrator, you provide reports to share information about role-based access control and compliance activities in the product. To provide reporting, CA Identity Governance integrates with CA Business Intelligence.

Important! For this release, install CA Business Intelligence 3.3 as the reporting engine. (BusinessObjects XI 3.1 SP5). For more information on installing CA Business Intelligence 3.3, see the CA Business Intelligence documentation.



Follow these steps:

1. Connect to the report server (see page 68).
2. Create a database connection to the report server (see page 68).
3. Configure permissions on the database connection object (see page 69).
4. Extract data for the reports (see page 70).

Connect to the Report Server

To integrate the product with CA Business Intelligence, connect to the report server and import default reports.

Follow these steps:

1. In the Portal, go to Administration, System Checkup, BusinessObjects Checkup.

   The BusinessObjects checkup screen appears.

2. Enter the credentials of the report server in this screen.

   When all credentials are set properly and the connection is established, the Connection field displays 'Successful'.

3. Click Start to load the BIAR file. The BIAR file contains all the default reports for the product.

   The connection is established and default reports are imported into the system.

Create a Database Connection to the Report Server

To allow the report server to access the reporting information in the database, create a database connection to the report server.

Follow these steps:

1. Log on to the system where you installed CA Business Intelligence.
2. Install the Client Software that is associated with your database (Microsoft SQL or Oracle).
3. Go to Start, Programs, BusinessObjects XI 3.1, BusinessObjects Enterprise, Start to start the Universe Designer.
4. Log in as an administrator.
5. Import the CA Identity Governance universe as follows:
   a. Go to File, Import to import a universe.
   b. Click Browse and Select CA Universes, CA Identity Governance.
   c. Select the CA Identity Governance universe under available universes.
   d. Click OK.
6. Define a new connection as follows:
   a. Go to File, Parameters.

      The Universe Parameters screen appears.

   b. Click New and Next to start the connection wizard.

c. Enter a connection name and select a driver as follows:
   - Microsoft SQL 2005 or 2008: OLE DB Providers
   - Oracle 10 or 11: Oracle Client

d. Provide database credentials.

e. Click Finish and click Test to test the connection.

f. Click OK.

   The Universe Parameters screen closes.

7. Save the universe and export the changes to the report server as follows:

   a. Go to File, and click Save.

   b. Go to File, Export.

   c. Click OK.

   The changes to the universe are successfully exported and the database connection object is created.

Configure Permissions on the Connection Object

Database connections are secure objects in the BusinessObjects server, so add permissions to access the connection object.

Follow these steps:

1. Log on to the BusinessObjects Central Management Console at the following URL:

   http://*businessobjects_hostname*:8080/CmcApp

   Note: 8080 is the default HTTP port. If you selected a different port during installation, use it here.

2. In the drop-down list, select Connections.
3. Right-click the connection that you created and select User Security.
4. Click Add Principals.
5. Select the CA Identity Governance group and click the arrow to move it to the right.
6. Click the Add and Assign Security button.
7. Add the View and View On Demand access and Click OK.
8. Click Close.

Extract Data for Reports and Dashboards

Gather the data for the reports (or dashboards) available in the Portal. To populate the data, run an ETL process that extracts the data you specify, transforms the data to fit operational purposes, and loads the data into the database.

Follow these steps:

1. In the Portal, go to Administration, Manage the ETL Process.
2. Select the universe for the ETL process.
3. Select the entity attributes you want to extract before running the ETL process.

   Note: By default, all attributes are selected. For performance reasons, only select the attributes you need to extract.
4. Click Run ETL to run the process immediately, or click Schedule ETL to schedule the process.

Create Custom Reports

If you want to report on different information than what is available in the default reports, create custom reports and run them in the product.

Follow these steps:

1. In the Portal, go to Reports, Manage Reports.
2. Log in to InfoView.
3. Click Document List and expand Public Folders.
4. Navigate to CA Reports, CA Identity Governance.
5. Right-click the CA Identity Governance folder and select New, Web Intelligence Document.
6. Double-click the CA Identity Governance Universe.

   Note: Do not install the samples to avoid having unneeded universes.
7. Build the report using the CA Identity Governance objects provided.

   Note: For more information on building reports, see the BusinessObjects documentation.
8. Click Run Query.
9. Adjust report format and styling.

10. Click Save and browse to Public Folders, CA Reports, CA Identity Governance.
11. Type the name of the report and click OK.

    Your report is saved and now appears in the Portal under Reports, View Reports.

Note: Be sure that the user running the custom report has the appropriate permissions to view the report in the product.

Chapter 8: Business Workflows

A *business workflow* is a set of related tasks that fulfill a business requirement, such as certifying user privileges, or requiring approvals for privilege changes.
Business workflows implement a company's procedures for determining compliance with internal and external policies in CA Identity Governance. Implementing these procedures in CA Identity Governance can help ensure that a company has a reliable and repeatable method for validating compliance.

For example, a company wants to perform a quarterly audit of their employees' access to company resources. The compliance officer initiates a certification that requires managers to certify the privileges of their direct reports. The compliance officer further requests that resource owners approve any rejected privileges for the resources they manage. In this example, the certification and approval steps comprise a business workflow. The company can initiate that workflow on a quarterly basis, or more frequently, as required.

You can define business workflows for the following activities:

- Certifications
- Self service requests, such as a manager requesting a privilege change for an employee, or requesting a change to roles that they own

  Note: Self service requests are initiated through the Role Management tab in the Portal.
- Approval requests for changes to the role model made through the DNA client tools

Note: This online help system only provides details about the workflow screens in the Portal. Administrators who are responsible for configuring CA Identity Governance can view additional information about business workflows in the *Configuration Guide* in the CA Identity Governance bookshelf.

This section contains the following topics:

Administer Business Workflows (see page 74)
Monitor Workflow Progress (see page 76)
Start and Stop Workflows (see page 77)
Define and Send Escalation Emails (see page 77)

Administer Business Workflows

Administrators use the workflow screen to track and control certifications and other active workflows.

To administer business workflows

1. In the CA Identity Governance Portal, go to Administration, Workflows.

   The screen lists the active workflows. When a workflow concludes, it is removed from the list.

2. (Optional) customize the information fields displayed in the table.

3. (Optional) Filter the workflows displayed in the table (see page 75).

4. Click a workflow to view its details.

   The workflow detail screen appears. It contains the following tabs:

   - Overview - a dashboard that shows the progress of the flow in graphs and charts. This tab is open by default.
   - Administration - provides advanced workflow control options to stop or restart the workflow, or to send escalation emails (see page 77) for incomplete actions.
   - Workflow Progress by Affected Entities - lists tasks by the entities under review in each task, and shows their progress.
   - Workflow Progress by Reviewers - lists actions by their reviewers, and shows their progress.

5. Manage workflow tasks and actions in detail:

   a. Click one of the Workflow Progress tabs.

      Actions are listed in groups. The table shows the progress of each group.

      Note: When the scope of the workflow is large, or additional large workflows are active, the progress bars may not update immediately. It may take several minutes for submitted actions to be counted as complete in the progress bars.

   b. Click the Open button next to a group.

      A table lists actions in the group.

   c. Click the Open button or the Reviewers icon to view more detail.

   An action details screen displays an action or group of actions of one type, from one workflow, related to one primary entity.

   Actions that are already submitted to CA Identity Governance are dimmed.

6. Use the information fields and interactive options of the screen to review links.

   Only Reassign, Comment, and Attachment operations are available for actions that are assigned to others.

   Approve and Reject options are available only for actions that are assigned to you.

7. Do one of the following:

   - Click Submit to submit your decisions to CA Identity Governance.
   - Click Cancel to return to the overview screen without saving your decisions.

Filter the Workflow List

You can filter the list of workflows to help you find specific workflows or groups of workflows.

To filter the workflow list

1. Click Filter in the page header.

   The Filter Workflows dialog appears.

2. Define filter criteria as follows:

   Due Date

   Use the From and To fields to specify a time period. The filter selects workflows with a due date within that period.

   Workflow Types

   Select the types of workflows to display. Select the All option to select all types of workflows, or to clear your selection.

   Workflow States

   Select the states of workflows to display. Select the All option to select all states, or to clear your selection. The filter selects workflows that are currently in the specified states.

   Note: You can combine these filter criteria.

3. Click OK.

   The list displays only workflows that meet your filter criteria.

Monitor Workflow Progress

Workflow owners can monitor the progress of a workflow process that they initiate by using the Overview tab in a workflow details screen. Users access the Overview tab by opening Administration, Workflows, and selecting a workflow process to view its details.

The Overview tab displays workflow progress in charts. You can view progress in each chart as a percentage or as a value by selecting the appropriate option above each chart. If you select Value, CA Identity Governance displays workflow progress based on the number of completed tasks in the workflow.

To update the chart to reflect the current status without reopening the Overview tab, click Draw Chart.

Note: To view additional details about tasks in a workflow progress, use the Workflow Progress by Reviewers and the Workflow Progress by Entities tabs (see page 76).

View Workflow Progress by Entities or Reviewers

The My Requests and Certification screens present two ways to view the progress of a workflow.

- The Workflow Progress by Affected Entities tab groups items of the workflow by the entities under review in each item. The entries in these tables are items generated by the product for the workflow, based on the workflow type, base configuration, scope of entities under review, and other settings.
- The Workflow Progress by Reviewer tab groups items of the workflow by the reviewer to whom they are assigned, and shows their progress. The entries in these tables are actions generated by the Workpoint jobs that implement items of the workflow.

When a workflow is in progress, you can drill down from either tab to view individual actions. The Workflow Progress by Affected Entities tab displays high-level items created by the product. The main views of this tab are populated when the product completes its analysis of the links under review in the workflow.

Each of these items spawns many Workpoint jobs when they are implemented. The Flow Progress by Reviewer tab displays the resulting low-level Workpoint jobs, and the reviewers that were assigned to each link. This tab is populated only when Workpoint jobs are initiated, and its contents depend on the logic implemented for each task by the corresponding Workpoint process.

Start and Stop Workflows

You can manage business workflows in the Administration tab of the Workflows screens, which are located in the Administration Menu. The Administration tab lets you review general workflow information, and start, stop, and archive a workflow. This tab contains the following options:

Start Workflow

Launches a certification.

Stop Workflow

Suspends a workflow. Actions of this workflow appear in the queues of participants, but Approve, Reject, and Reassign options are not available. Changes resulting from certification decisions are no longer exported to provisioning endpoints.

Note: You cannot restart a workflow after you stop it.

Archive

Removes the workflow from all queues, and stores the current state of the workflow. Changes resulting from certification decisions are no longer exported to provisioning endpoints.

Escalation Emails

Allows you to define and send reminder emails (see page 77) during a certification. This option is only available for certification workflows.

Define and Send Escalation Emails

Administrators can configure CA Identity Governance to send emails to remind reviewers to complete their tasks for a certification.

To define and send escalation emails

1. In the CA Identity Governance Portal, go to Administration, Workflows.
2. Select an active workflow.
3. Under the Administration tab, click Escalation Emails.

   The Escalation Emails pop-up appears.

   Note: The Escalation Emails button appears for certifications only.
4. Configure the following information for the emails you want to send:
   - Send criteria—percentage of work done by a specific time relative to the due date
   - Email Template—template to use for the sent email

- Recipient Type—Accountable, Email Address, or Member List
- Recipient—dynamic options dependent on recipient type

5. Add more email definitions if necessary. Click the plus (+) icon. To remove email definitions, click the X icons.
6. Click *one* of the following:
   - Load

     Loads a different definition set. This option allows you to switch between different definition sets for editing.
   - Save

     Saves the current definition set.
   - Send Now

     Escalation emails are immediately sent to reviewers to remind them to complete their tasks.
   - Schedule Emails

     Schedules emails to be sent to reviewers at regular intervals.

Chapter 9: How to Perform Data Transformations

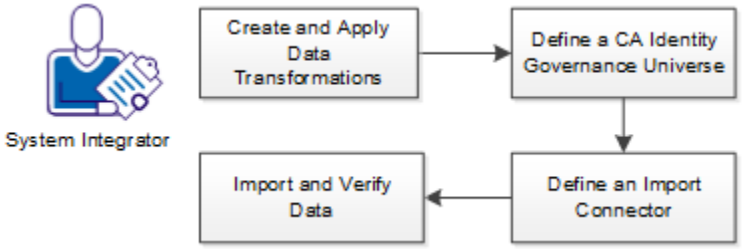
Introduction

CA Identity Governance uses built-in connectors to work with endpoint data types. Use data transformation to manipulate data before you import it into CA Identity Governance, or if your endpoint systems cannot use the built-in connectors.

Data transformation enables you to perform advanced data manipulation and automate imports of data from various endpoint systems. When you perform a data transformation, you convert a set of data values from the data format of your endpoint system into a data format that CA Identity Governance uses.

CA Identity Governance includes the third-party open source product Pentaho Data Integration (also known as PDI, or Kettle). This utility enables you to create, run, and automate complex ETL (Extract, Transform, and Load) operations during data import. You can perform and automate the ETL operations with relative ease using PDI, batch processing (SBT), and the Portal custom connectors.

The following diagram outlines the steps that you follow to create and apply transformations:



Follow these steps:

1. Create and apply data transformations (see page 80).
2. Define a CA Identity Governance universe (see page 85).
3. Define an import connector.
4. Import and verify data (see page 93).

Create and Apply Data Transformations

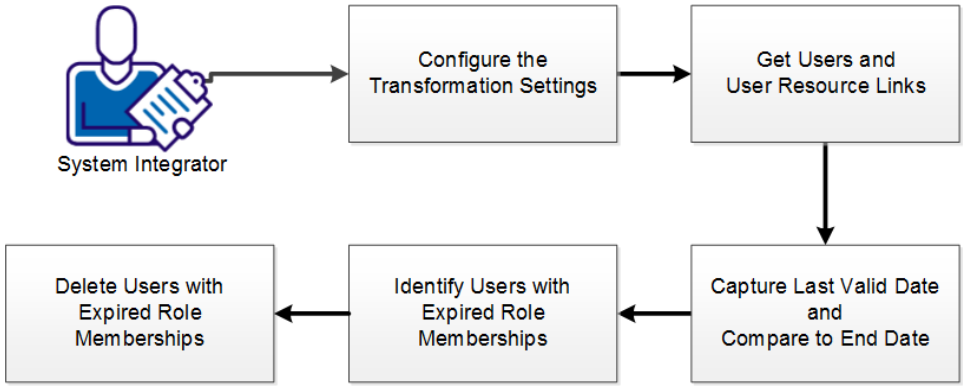
As a systems integrator, you add or modify CA Identity Governance data. You can modify data during an import (or an export) by running a transformation.

Use Case - Remove Expired Links

You are importing data from an Enterprise Resource Planning (ERP) application. In this application, users have roles membership. When the role membership of a user expires, CA Identity Governance maintains the account record and adds an end date value. When you import the data into CA Identity Governance, you can filter out users with expired role memberships based on the end date. This filter ensures that managers do not certify invalid access during a certification.

Note: This scenario outlines the steps to create the transformation sample KTR file **removeExpiredUserResourceLinks.ktr** that is located in the CA\RCM\Server\data-integration\samples\RCM directory. In this scenario, we remove expired links to SAP or Oracle roles that are modeled as resources in CA Identity Governance.

In PDI, a transformation comprises a series of steps. Each step represents an action that is performed on the data. A hop represents a data pathway that connects the steps and enables schema metadata to pass from one step to another.



Follow these steps:

1. Configure the transformation settings. (see page 81)
2. Get users and user-resource links (see page 82).
3. Capture last valid date and compare to end date (see page 83).
4. Identify users with expired role memberships (see page 83).
5. Delete users with expired role memberships (see page 84).

Configure the Transformation Settings

For your transformation to connect to CA Identity Governance, configure the transformation settings in PDI.

Follow these steps:

1. Launch PDI, as follows:
   - **Windows:** Go to **Start**, **Programs**, **CA**, **Role & Compliance Manager**, **Server**, **Data Integration Tool (PDI)**.
   - **Linux:** Click the **Data Integration Tool (PDI)** icon in your home directory.

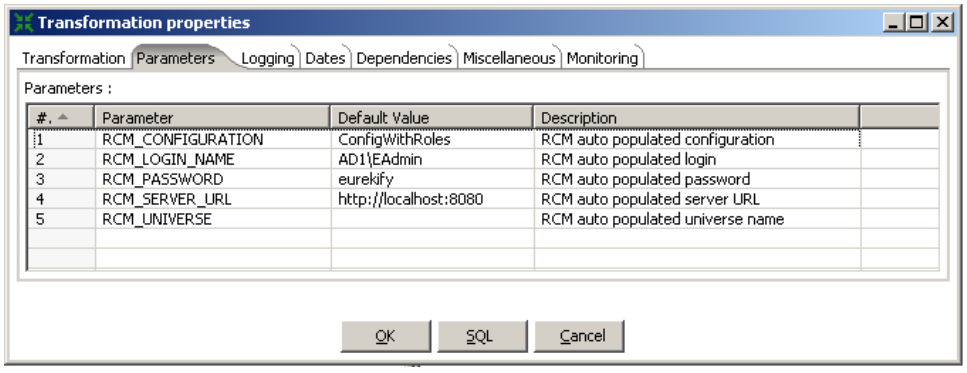
   Note: PDI is located in the following directory:

   `CA\RCM\Server\data-integration`
2. Go to **File**, **Open**, and browse to the following directory:

   `data-integration\samples\RCM`
3. Open the **template.ktr** file and save it under another name that is relevant to the transformation you want to create.
4. Press **CTRL-T**.

   The **Transformation properties** windows opens.
5. Click the **Parameters** tab, and enter the following CA Identity Governance information:
   - RCM_CONFIGURATION
   - RCM_LOGIN_NAME
   - RCM_PASSWORD
   - RCM_SERVER_URL
   - RCM_UNIVERSE

   The following image is an example of the Parameters field with example server information:



6. Click **OK**.

   You have started PDI and configured the CA Identity Governance settings.

Now that PDI is configured, you can define the steps in your transformation.

Get Users and User Resource Links

To identify expired links, locate CA Identity Governance users, and obtain the user-resource links for users that have the start and end date information, use **Get Users and Links.**

Follow these steps:

1. In PDI, select and drag the **Input Users** step to the Transformation screen in the **Design** tab, under **RCM Input**.
2. Right-click the step and select **Edit step**.

   The I**nput Users!** window opens.
3. Under the **Fields** tab, click **Get fields**.

   All the available fields are populated.
4. Delete all fields except **PersonID**, and click **Ok**.
5. Select and drag the **Get User-Resource Links by Users** step to the Transformation screen in the **Design** tab, under **RCM Links**.
6. Right-click the **Get User-Resource Links by Users** step and select **Edit step**.
7. Under the **Link Fields (Keys and Attributes)** tab, click **Get Link Fields**.
8. Delete all fields except the following, and click **Ok**:
   - PersonID
   - ResName1
   - ResName2
   - ResName3
   - Start Date
   - End Date
9. Create a hop between the **Input Users** step and the **Get User-Resource Links by Users** step.

   You have added the step to Get Users and Links.

Capture Last Valid Date and Compare to End Date

To identify expired role memberships, add a field to define the last valid date when you run the transformation. The transformation filter compares this last valid date to the role membership end date to filter out users with expired role memberships.

Follow these steps:

1. In PDI, in the **Design** tab, locate and expand the **Transform** step, select **Add constant**, and drag it to the Transformation screen.
2. Right-click the **Add constants** step and select **Edit step**.
3. Add a field that is named '**LastValidDate' of type 'String**', and click **Ok**.
4. Create a hop between the **Get User-Resource Links by Users** step and the **Add Constants** step.
5. Click the **Transform** tab, select the **Set field value to a constant** step, and drag it to the Transformation screen.
6. Create a hop between the **Add constants** step and the **Set field value to a constant** step.
7. Right-click the **Set field value to a constant** step and select **Edit step**.

   The **Set field value to a constant** window opens.
8. Select the **Use variable in constant** option, and click **Get fields**.
9. Add the **LastValidDate** field and set the **Replace by value** field as follows:

   `${Latest_Valid_Date}`

   You provide this date when you run the transformation.
10. Click **Ok**.

    You have added a field to define the last valid date when you run the transformation.

Identify Users with Expired Role Memberships

To ensure that managers do not certify invalid role memberships, filter out users with expired role memberships based on the end date.

Follow these steps:

1. In PDI, in the **Design** tab, locate and expand the **Flow** step, select **Filter rows**, and drag it to the Transformation screen.
2. Right-click the **Filter rows** step and select **Edit step**.

3. In the **Filter rows** window, set the destinations steps as follows:
   - **Send 'true' data to step:** Text file output
   - **Send 'false' data to step:** Dummy (do nothing)
4. Create the following condition in **The condition** box:

   ```
   End Date < LastValidDate
   AND
   End Date IS NOT NULL
   ```

   This condition compares the **End Date** with the **LastValidDate**. If the **End Date** occurred before the **LastValidDate**, the link has expired.
5. Click **Ok**.

   You have created a filter to identify users with expired role memberships based on a defined end date.

   You have added the output steps to identify users with expired role memberships. When you run the transformation, it identifies all users with expired role memberships.

Delete Users with Expired Role Memberships

To ensure that managers do not certify invalid role memberships, delete users with expired role memberships based on the end date.

Follow these steps:

1. In PDI, in the **Design** tab, locate and expand the **Flow** step, select **Dummy (do nothing)**, and drag it to the Transformation screen.
2. Create a hop between the **Filter Rows** step and the **Dummy (do nothing)** step.

   All valid links are sent to the **Dummy (do nothing)** step.
3. Select **Text file output**, and drag it to the Transformation screen.
4. Right-click the **Text file output** step and select **Edit step**.

   The **Text file output** window opens.
5. Under the **File** tab, provide a filename for the text output file.
6. Under the **Fields** tab, click **Get Fields**.
7. Delete all fields except for the following and click **Ok**:
   - PersonID
   - ResName1
   - ResName2
   - ResName3

- Start Date
- End Date

8. Create a hop between the **Filter rows** step and the **Text file output** step.

   All users with expired links are captured and sent to the Text file output.

9. On the **Design** tab, locate and expand the **RCM Output** step, select the **Delete User-Resource Links** step, and drag it to the Transformation screen.

10. Right-click the **Delete User-Resource Links** step and select **Edit step**.

    The **!Delete User-Resource Links!** window opens.

11. In the **General** tab, in the **RCM Configuration** section, map the following fields, and click **Ok**:

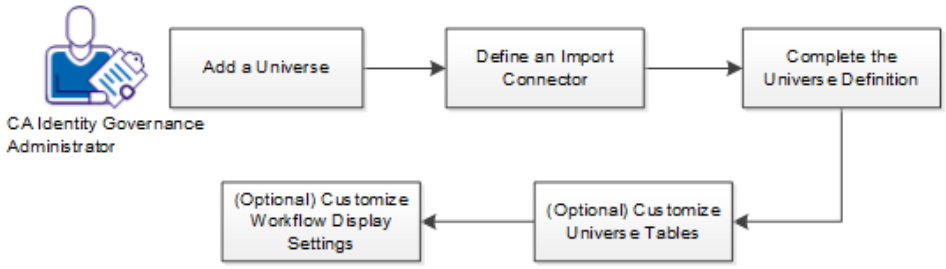
    - Person ID Field=PersonID
    - Res Name 1 Field=ResName1
    - Res Name 2 Field=ResName2
    - Res Name 3 Field=ResName3

    You have added the output steps to delete users with expired role memberships. When you run the transformation, it deletes all users with expired role memberships.

How to Define a Universe

This scenario describes how to define a CA Identity Governance universe.

The following diagram outlines the steps that are required to define a CA Identity Governance universe:



Follow these steps:

1. Add a universe (see page 86).
2. Define an import connector.
3. Complete the Universe definition.
4. (Optional) Customize universe tables.
5. (Optional) Customize Workflow display settings.

Add a Universe

To create a universe in CA Identity Governance, note the names of the Master and Model configurations and determine audit settings. The Master and Model configurations and the audit settings affect universe behavior. Master and model configurations are unique for each universe. Do *not* create more than one universe that uses the same master or model configuration. Examples of configuration file names: *XX*_master.cfg, *XX*_model.cfg

Note: Configuration file names cannot contain slash ("/" or "\") characters.

Follow these steps:

1. In the **Portal**, go to **Administration**, **Universes**.
2. Click **Add New**.
3. Provide values for mandatory fields:

   Note: An orange dot indicates a mandatory field.

   Master Configuration name

   Defines the configuration that is an image of the privilege model exactly as it is on the target system.

   Model Configuration name

   Defines the configuration that is an image of the privilege model as CA Identity Governance prefers to be.

Audit Settings File

Specifies the parameters and settings that define the audit and pattern-based checks that are performed on the master configuration at the end of the import.

These parameters and settings specify which pattern and Business Policy Rules (BPR) checks are run. A BPR expresses business, provisioning, or security constraints as a logical condition that can be applied to the entities and links in a CA Identity Governance configuration. For example, a new link between a user and a resource violates a certain predefined BPR rule. If the BPR in which the rule is written is in the audit setting file, it is tested at the end of an import and an alert is raised.

Note: When you create multiple universes, it is good practice to use a custom audit settings file. This approach enables you to tailor the audit settings file to each specific universe. You also reduce the number of unnecessary alerts by defining a BRP file that is specific to the universe.

Follow these steps:

1. Navigate to the CA\RCM\Server\eurekify-jboss\conf\audit directory
2. Open the **default-parameters.properties** file in a text editor.
3. Click File, Save As, and save the file in the CA\RCM\Server\eurekify-jboss\conf\audit directory with a name that identifies the universe you want to use.
4. In the Portal, Add New Universe screen, select the new file instead of the default audit settings file.
5. Click **Save**.

4. Click **Save**.

Next, define an import connector.

Define an Import Connector

A connector retrieves data from one or more target systems. Connectors assemble the privilege model from objects such as accounts, groups, resources, and other system-specific objects. CA Identity Governance import connectors import data from endpoint systems. To define an import connector, use the import connector wizard under the connectivity tab of the universe. The wizard guides you through mapping users, roles, resources and accounts to CA Identity Governance.

Follow these steps:

1. In the CA Identity Governance **Portal**, **Administration**, **Universes**, select the universe that you created to import the data.
2. Select the **Connectivity** tab.
3. Select **Import** and click **Add Connector**.

4. In the Connector wizard, provide values for all mandatory connector settings.

   Note: For specific connectors, additional steps are necessary. For more information, see the *Configuration Guide.*

5. Click **Finish**.

   The new import connector is defined in CA Identity Governance.

6. (Optional) Select the new connector and click **Validate**.

   This step confirms that the import connector is defined correctly and is ready to retrieve data from the target system.

   You have validated the connector parameters and configuration.

Note: CA Identity Governance automatically defines a matching export connector for every import connector that you define.

Next, complete the universe definition.

Complete the Universe Definition

Navigate to the General tab and continue to define the Universe by providing values for optional fields. These fields configure user, role, and resource variables for the universe.

1. In the **Administration**, **Universes**, **General** tab, enter values for the following fields:

   Configuration Users Login Field

   Specifies the field in the user database that maintains the user login field for logging in to the Portal.

   Note: AnyExecutable, PDI and SBT are third-party external components that are currently unavailable.

   Configuration Users Email Field

   Specifies the field in the user database that maintains the login name for logging in to the Portal.

   Configuration Users Manager Field

   Specifies the user manager ID field in universe configurations (user approver).

   (Optional) Configuration Users Display Name Field

   Specifies which field acts as the default table link to the Details popup dialog. This dialog appears when no field is selected as the Details field.

   Note: For more information about the Details popup dialog, see the *Administration Guide*.

   Configuration Roles Manager Field

   Specifies the role manager ID field (role approver) in universe configuration files.

(Optional) Configuration Roles Display Name Field

Specifies the field in the user database that maintains the roles for a universe. This field acts as the default table link to the Details popup dialog that appears when no field is selected as the Details field.

Configuration Resources Manager Field

Specifies the field in the database configuration that maintains the resources manager ID used to approve a resource.

(Optional) Configuration Resources Display Name Field

Specifies the field in the database configuration that maintains the resources for a universe.

(Optional) Configuration Resources Description Field

Specifies the field in the database configuration that maintains the resource descriptions for a universe.

(Optional) Configuration Resources Application Field

Specifies the ResName (resource name) field in the database configuration that identifies the endpoint or source application of a resource. This field usually maps to the endpoint or application group of the resource.

Note the following:

- For more information about the resource database file, see the *Programming Guide*.
- When integrating with CA Identity Manager or using the CA IAM CS, ResName2 is used. Use this field to define the application during CA User Activity Reporting integration. For more information about integration between CA Identity Governance and CA Identity Manager, see the *Configuration Guide*.

(Optional) Approved Audit Card

Defines the list of Universe violations which are added during normal system activity.

Note: For more information about Audit Cards, see the *Configuration Guide.*

(Optional) Approved alerts are

Specifies whether pre-approved violations are ignored (hidden) or unavailable (dimmed) in CA Identity Governance portal.

Audit Settings File

Specifies parameters and settings that define the audit and pattern-based checks that are performed on the master configuration each time an import occurs.

High Risk Threshold

Defines the value that is used to categorize high risk warnings in a certification. If a violation of a business policy rule with a score value that is equal to or greater than this threshold value occurs, a high risk warning is displayed in the certification.

Default: 90

Medium Risk Threshold

Defines the value that is used to categorize medium risk warnings in a certification. If a violation of a business policy rule with a score value that is equal to or greater than this threshold value occurs, a medium risk warning is displayed in the certification.

Default: 60

2. Click **Save**.

   Next, customize universe tables for configuration data.

(Optional) Customize Universe Tables

For each universe, you customize the table layout that the entity browser and role management screens use to display the configuration data. This modification enables you to determine how to display information and select mandatory columns. You can set table column order, composition, and lock columns.

Note: A blue lock icon in the locked position displayed in the Entity Browser - Display Settings screen indicates a displayed column that can be moved (order). The locked column cannot be deleted. Each table must always have at least one member.

Follow these steps:

1. In the CA Identity Governance **Portal**, go to **Administration**, **Universes**.
2. Click **Edit** next to the universe that you want to edit.
3. Select the **Entity Browser - Display Settings** tab.

   This tab contains table header views. The Users, Roles, and Resources views display the layout of each entity table in the entity browser.

4. Customize the table layout as follows:
   a. Click **Customize** on the table header that you want to modify.
   b. Use the arrow icons to add, remove, or order available fields (columns).

      Note: System parameter table.default.rowsPerPage (see page 91) enables you to set displayed rows for a table

c. Customize the columns and click **OK**.

d. Click the lock icon (open position) next to the column name to make the column mandatory (locked position). In the Entity Browser, when customizing, users can move a mandatory column in the display order, but they cannot remove it from the display.

5. Click **OK**.

   The entity browser displays universe configurations in the table formats that you specified.

   Next, you can customize workflow display settings.

Set the Default Rows Per Page

You can specify the default number of rows that appear in a table by using the table.default.rowsPerPage system property.

Note: This system property applies only to tables with the Customize feature.

table.default.rowsPerPage

Overrides current rows per page (usually 10), use -1 to retain system default.

(Optional) Display Attribute as a Hyperlink

Hyperlinks simplify navigating entity attributes. To use this feature, Enable the linked attributes property and configure the universe to display linkable attributes in the Entity Browser and the entity bubbles that pop up in the certification tasks view.

Follow these steps:

1. Click Administration, Settings, Property Settings.
2. Locate the **linkable.properties.enable** attribute and click the Edit icon.
3. Set the Property Value to **True**, set the Type to **Database Property**, and click Save.

   You have enabled the **linkable.properties.enable** property.
4. Click Administration, Universes, and click the universe that you want to modify.
5. Select the Entity Browser – Display Settings tab.
6. Click the web-link icon next to the attributes that you want to appear as hyperlinks, and click OK.

   Note: The **linkable.href.format** property uses regular expressions to validate the hyperlink. The most typical linkable attributes are email addresses and URLs. The default regular expression matches any valid URL that begins with mailto, news, http, https, ftp, and ftps. To customize hyperlink validation, add protocols to the **linkable.href.format** property.

(Optional) Customize Workflow Display Settings

For each universe, you can customize the table layout that the product uses to display workflow views.

Note the following:

- A red lock icon displayed in the Workflow Display Settings screen indicates a mandatory displayed column (system default). Such columns can be moved (order). Administrators can define additional mandatory columns.
- A blue lock icon in the locked position displayed in the Workflow Display Settings screen indicates a displayed column that you can move (order), but cannot delete.

Follow these steps:

1. In the **Portal**, go to **Administration**, **Universes**.
2. Click **Edit** for the universe that you want to edit.
3. Select the **Workflow Display Settings** tab.

   This tab contains table header views displayed in the certification screens. The General, User, Role, and Resources Actions headers display the table layouts for the screen.
4. Customize the table layout as follows:
   a. Click Customize on a table header that you want to modify.
   b. Use the arrow icons to add, remove and order the columns.
   c. When you finish customizing the columns, click OK to close the Customize window.
   d. In the Workflow Display Settings window, click the lock icon next to the column name to make the column mandatory. Users can move a mandatory column, but they cannot remove it.
5. Click **OK**.

   The product displays tables in the format that you specified.

Import and Verify Data

As a systems integrator, you may need to enrich or modify data within CA Identity Governance. You can modify data during an import (or an export) by running a transformation.

Follow these steps:

1. In the **Portal**, go to **Administration**, **Universes**, select the desired universe, and click on the **Connectivity** tab.
2. Select the desired connector and click **Import Now**.

   A confirm Run Import window appears.
3. Click **OK**.

   The data import begins.
4. To view the import status progress, go to **Administration**, **Workflows**.

   The Workflows are displayed.
5. To view workflow progress details, click the desired workflow.
6. Check that the data is properly loaded through the Portal Entity Browser or inspect the imported configuration in the Client Tools.

Chapter 10: System Maintenance

This section contains the following topics:

Repair CA Identity Governance Configuration, User, and Resource Files (see page 95)
Purge Data (see page 96)

Repair CA Identity Governance 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.

To repair CA Identity Governance configuration, user, and resource files

1. In the CA Identity Governance Portal, go to Administration, Settings, Fix Configuration.

   The Fix Configuration screen appears.

2. Select a configuration file from the drop-down list and click Analyze.

   CA Identity Governance 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 Identity Governance 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.

Purge Data

Good management practice requires you to purge old, unneeded data files from the CA Identity Governance database server periodically. The purge utility simplifies this maintenance task.

Important! Purging removes data completely and permanently from CA Identity Governance databases. Back up all data before you purge, and verify that the data you purge is unnecessary.

The purge utility enables you to purge data in the following ways:

- Purge by Document—Delete selected documents and data files. Using this utility, you can delete the following documents and data files:
  - Certifications
  - Import/Export/Correlation Process (workflow)
  - Configuration

  - Universe
  - Approval Process (workflow)
- Purge by Date—Clear the database or system logs of entries older than a specified date.
- Purge Permissions Configuration Users—Remove inactive Portal users who are not associated with at least one universe.

Purge by Document

Use the Portal purge utility to delete outdated or unneeded data files from the CA Identity Governance database.

Important! Purging removes data completely and permanently from CA Identity Governance databases. Back up all data before you purge, and verify that the data you purge is unnecessary.

When you delete a universe or configuration file, the following associated files are also deleted:

- Related configuration files such as master, model, and RACI configurations.
- Audit Cards
- Certifications
- Log Entries
- Member Lists

Note: **You need administrator-level rights in the Portal to perform this procedure.To purge documents**

1. In the CA Identity Governance Portal, go to Administration, Settings, Purge Data.

   The Purge Data screen appears.
2. Select the By Document option in the Purge Type drop-down list, and click Next.
3. Select the type of document you want to purge in the Document Type drop-down list and click Next.

   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.
5. Click Next.

   The Confirmation screen appears.

6. Review the scope of the data purge, as follows:
   - In the Document Types area, expand the tree to view the data files selected for the 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 selected for the 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 Identity Governance database. When the purge is complete, a confirmation message appears in the Purge Data screen.

Purge by Date

Use the purge utility to delete transaction (Tx) log entries or portal usage tracing data that is older than a specified date.

Important! Purging removes data completely and permanently from CA Identity Governance databases. Back up all data before you purge, and verify that the data you purge is unnecessary.

To purge data by date

1. In the Portal, go to Administration, Settings, Purge Data.

   The Purge Data screen appears.
2. Select the By Date option in the Purge Type drop-down list and click Next.

   The Selection Type screen appears.
3. Select the type of data you want to purge in the Select Type drop-down list 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 deleted.

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 Identity Governance 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.

8. Click Purge.

   The specified data is completely and permanently deleted from the CA Identity Governance 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 access the Portal to participate in certifications, and to use self-service role management tools. Each user must have a Portal user account. The product creates these user accounts automatically based on retrieved user data. The *permissions configuration* file (eurekify.cfg) stores the Portal user account information.

To preserve data integrity and the security of the Portal, remove users who no longer require access.

The purge utility automatically identifies portal users who are not affiliated with an existing universe. These users cannot participate in any processes, and are candidates for deletion.

Important! Purging removes data completely and permanently from CA Identity Governance databases. Back up all data before you purge, and verify that the data you purge is unnecessary.

Follow these steps:

1. In the Portal, go to Administration, Settings, Purge Data.

   The Purge Data screen appears.

2. Select the Permissions Configuration User option in the Purge Type drop-down list and click Next.

   The CA Identity Governance 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 Identity Governance database. When the purge is complete, a confirmation message appears in the Purge Data screen.

Purge Workpoint Jobs Associated with a Workflow

CA Identity Governance uses Workpoint to monitor and control business workflows by creating a certification item for each privilege in a certification.

To reduce the Workpoint database size, delete Workpoint job records for completed workflows.

Follow these steps:

1. Open an SQL command prompt, connect to the Workpoint database, and run the following command:

   ```
   update WP_PROCI set LU_ID = 'Delete Job' where PROC_STATE_ID = 5;
   ```

   This command marks all completed jobs for deletion.

2. Execute the following command:

   ```
   execute spWP_DELETE_JOBS;
   ```

   This command deletes the marked jobs.

   You have marked and deleted completed jobs on the Workpoint database.

Chapter 11: Troubleshooting

This chapter provides a list of the CA Identity Governance Portal Error Messages

This section contains the following topics:

Trace Workflow (see page 103)
Error Messages (see page 103)
Resources Do Not Appear in BPR Drop-down List (see page 112)
Using the Pipe Character (|) in Regular Expressions (see page 113)
Property: bpr.sod.ignore.zero (see page 113)
Property: bpr.all.representative (see page 114)
System Checkup (see page 114)

Trace Workflow

As an administrator, you want to view details and events that relate to a workflow process. These details can help you understand what is happening during a particular process, or can help you troubleshoot a problem with the process.

To trace workflow information, go to Administration, Workflows, select the Administration tab and click Show all Events, then click Show Workflow Trace. This option adds a Workflow Trace tab to the Workflow screen that displays all the messages associate with the current workflow.

Error Messages

CA Identity Governance contains messages that are 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 error 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.

Field	Code	Description
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 ${maximum} characters long.
stringvalidator.minimum.errcode	app009	'${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

Field	Code	Description
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	select at least one option for ${byfield} field.
configurationname.required.errcode	arp002	select a configuration.
campaignname.required.errcode	arp003	select a campaign.
byfield.required.errcode	arp004	select the 'by field' parameter.
auditcard.required.errcode	arp005	select audit card.
sort.required.errcode	arp006	select sorting method.
campaignfilteroption.required.errcode	arp007	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}.

Field	Code	Description
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.
settings.strings.ie.errors.missingmaxduration.errcode	cst009	missing maxduration field.
settings.strings.ie.errors.errorparsingmaxduration.errcode	cst010	error parsing maxduration field, 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	enter all auditcard names
dashboard.compliance.error.multiname.errcode	dbc002	name {0} appears more than once
dashboard.compliance.error.nocard.errcode	dbc003	enter all audit cards
dashboard.compliance.error.multicard.errcode	dbc004	auditcard {0} appears more than once
dashboard.compliance.error.nobpralerts.errcode	dbc005	auditcard {0} has no bpr alerts
entity.emptylist.errcode	eml001	no match was found
mail.builder.createticket.sage.errticket.subject.errcode	mal001	new error ticket, title:{3}
mail.builder.createticket.sage.errticket.body.errcode	mal002	an 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, 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, 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.

Field	Code	Description
loginpage.userauthorization.failed.errcode	prt010	failed to authorize user: {0}, the user does not exist in {1} configuration.
internalerrorpage.label.info1.errcode	prt011	an error has occurred. For more information, view the log file.
internalerrorpage.label.info2.errcode	prt012	to relogin click here
sagemaster.headers.foundconflicts.errcode	sgm001	error! conflicts in the master configuration login field.
sagemaster.headers.countduplicates.errcode	sgm002	found {0} duplicate logins. 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.reject ed.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 .failed.errcode	tkt006	request to add resource {0} to user {1} - failed.

Field	Code	Description
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.e rrcode	tkt015	request to add role {0} to role {1} - rejected.
changeapproval.child.add.role.role.info.title.failed .errcode	tkt016	request to add role {0} to role {1} - failed.
changeapproval.child.add.role.role.info.description .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.description .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.tile .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}
changeapproval.child.remove.role.role.info.title .rejected.errcode	tkt021	request to delete role {0} from role {1} - rejected.

Field	Code	Description
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}
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}

Field	Code	Description
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, choose an accountable user to {0} role
changeapproval.child.remove.user.role.notification .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, fill the field name.
error.filter.errcode	tms007	the filter '{0}' has a syntax error. {1}
error.filter.resultempty.errcode	tms008	the user does not exist.
error.command.revokecmd.errcode	tms009	fail to revoke ticket {0}, missing job tickets {1}.
error.command.revokecmd.msg2.errcode	tms010	fail to revoke ticket {0} with job tickets {1}, there are {2} activity tickets outside the ticket tree.
error.command.linkcommands.errcode	tms011	fail to create commands:{0}, {1}
error.command.startjobcommand.errcode	tms012	fail to start job for ticket {0}, ticket has already reference for job {1}
error.command.startjobcommand.checkjobticketexists .errcode	tms013	fail to commit activity [checkjobticketexists] in job [{1}] of ticket {0}, check tms port in workpoint 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!

Field	Code	Description
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.optimisticlockexception .errcode	tms019	the ticket was updated by another user, reopen ticket.
error.validate.valuelength.errcode	tms020	validation fail for value:{0} cannot be longer than {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, view the log file.
page.internalerror.info2.errcode	tms028	null
page.expirederror.info1.errcode	tms029	your session has expired, 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}, watch log files.
text.dialogs.runfailed.errcode	txs002	failed to run {0}, watch log files.
settings.strings.universe.masterequalmodel.errcode	ust001	warning!!! master and model configurations are the same.
settings.strings.universes.errors.missingname .errcode	ust002	missing name field.
settings.strings.universes.errors.missingdescription .errcode	ust003	missing description field.
settings.strings.universes.errors.namealreadyexist .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.

Field	Code	Description
settings.strings.universes.errors.missingauditsettingsfile.errcode	ust007	was unable to find the audit settings file {0}.
settings.strings.universes.errors.masterisnotreadonly.errcode	ust008	the master configuration ({0}) is not read-only.
settings.strings.universes.errors.masterhasparent.errcode	ust009	the master configuration ({0}) has a parent configuration.
settings.strings.universes.errors.masternotlogged.errcode	ust010	the model configuration ({0}) is not logged.
settings.strings.universes.errors.modelisnotreadonly.errcode	ust011	the model configuration ({0}) is not read-only.
settings.strings.universes.errors.modelhasparent.errcode	ust012	the model configuration ({0}) has a parent configuration.
settings.strings.universes.errors.modelnotlogged.errcode	ust013	the model configuration ({0}) is not logged.
settings.strings.universes.errors.errorswasfound.errcode	ust014	the following issues were found:
settings.strings.universes.errors.wouldliketoautofix.errcode	ust015	would you like to auto-fix them?
error.workpoint.dbconnection.errcode	wp001	workpoint database connection is closed.

Resources Do Not Appear in BPR Drop-down List

If you have a long list of resources in CA Identity Governance, some resources do not appear in the drop-down list when creating or editing BPRs. To work around this issue, open the Client Tools, go to File, General Settings. Under the Files tab, increase the Maximum Item Count in Entity Name List.

Using the Pipe Character (|) in Regular Expressions

When you define regular expressions for Business Policy Rules in the Client Tools, you can specify the pipe (|) character to indicate a logical OR condition.

If you use the pipe character, enclose the values on both sides of the pipe character in parentheses. For example:

((value 1)|(value2))

If you do not include the parentheses around each value, CA Identity Governance can evaluate the rule in unexpected ways.

Property: bpr.sod.ignore.zero

Current Segregation of Duties (SoD) rules only consider users assigned to one or more of the specified resources. For this property, all users are considered, even those not assigned to resources.

The following property enables you to create an SoD rule that counts users that do not have any of the specified entities as violators.

bpr.sod.ignore.zero

True

Specifies that users who have no defined roles or resources on the left side of the SoD rule are not considered violators.

False

Specifies that users who have no defined roles or resources on the left side of the SoD are considered violators. The system detects users who have none of the specified entities.

Note: This functionality only exists in the CA Identity Governance Portal Client. Tools behavior is unchanged and ignores users with zero specified resources.

Default: True

Property: bpr.all.representative

This property controls the behavior of the ALL flag for BPR rules that specify their entities as regular expressions.

bpr.all.representative

True

Specifies that a representative entity for each rule is present.

False

Specifies that all of the entities that satisfy all of the rules are present.

Default: False

For example, if there are two rules on the left that say the following:

- Roles that begin with A
- Roles that begin with B

If the property is set to false, ALL is satisfied only if the user has all of the roles that begin with A and all of the roles that begin with B.

If the property is set to true, ALL is satisfied if the user has at least one role that begins with A (a representative that satisfies the first rule) AND at least one role that begins with B (a representative that satisfies the second rule).

System Checkup

Use CA Identity Governance system checkup tools to verify that messaging processes are working correctly.

The System Checkup option enables you to verify the following systems:

SMTP Checkup

Verify Simple Mail Transfer Protocol communication with an email server in the environment. The mail.smtp.timeout property default setting is 60 seconds.

Workpoint Checkup

Verify communication with the Workpoint server.

JMS Queue Checkup

Verify Java Message Service (JMS) communication.

SMTP Checkup

Simple Mail Transfer Protocol is used for email communications.

To verify SMTP communication

1. In the CA Identity Governance Portal, go to Administration, System Checkup, SMTP Checkup.

   The Checkup Options screen appears.

2. Enter a target email address.

3. Click Send.

   An email is sent to the target address from the sender specified in the 'mail.from' system property.

4. Verify that the email arrived.

Workpoint Checkup

Workpoint Checkup enables you to edit the TMS Workpoint adapter, view the Workpoint process list, and start a checkup ticket.

The Edit button enables you to edit the TMS Workpoint adapter that manages data communications with the Workpoint server. You can edit the TMS Property Value and Type in the Edit Property screen.

The Start button enables you to start a checkup ticket against the active processes displayed in the Workpoint process list.

JMS Queue Checkup

The JMS Queue Checkup enables you to test JMS connectivity. You can determine if you receive the message immediately, with a user-determined delay in seconds, or manual mode.