CA GovernanceMinder

Configuration Guide

12.6.02

CA Technologies Product References

- This document references the following CA Technologies products:
- CA GovernanceMinder
- CA IdentityMinder
- CA SiteMinder®
- CA User Activity Reporting
- CA SDM
- CA IAM Connector Server

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: Overview

This section contains the following topics:

Audience

This guide targets CA GovernanceMinder Implementors responsible for the product's configuration and behavior, and the product Integrators responsible for integrating the product with other CA products.

This guide details information about the following:

- Securing CA GovernanceMinder
- Importing data into the product
- Customizing CA GovernanceMinder behavior
- Customizing the look-and-feel of the product
- Setting Business Policies for compliance
- Integrations
- Performance tuning

It is assumed that the Implementor/Integrator is familiar with all the product components, the application server and operating systems they run on, and any other product information for which the product is integrating.

More information:

Security and Permissions (see page 73)

CA GovernanceMinder Universe Overview

A *universe* is a view into a management workspace that lets CA GovernanceMinder administrators manage entities such as users, roles, and resources collected from endpoints. Entity data is stored in configuration files. A universe contains a pair of master-model configurations, enabling the tracking of differences between the real-world configuration imported from the system (master) and the desired configuration generated (model).

Components of a Universe

A universe contains related configuration files and data files. Every universe contains the following configuration files:

- Master — A file that contains real-world user and user privileges information.
- Model — A file that starts as a copy of the Master configuration, but is updated to reflect any user privilege or role hierarchy changes.

  Note: All configuration files in a universe share a common structure. When you define a universe, you specify which fields store the unique ID, email, and other data for each user. These fields are used in CA GovernanceMinder certification, analysis, and report processes. All configuration files in the universe must comply with these field designations. For more information about configuration files, see the *Data Files appendix*.
- RACI — Four files created after analyzing the Model configuration file to determine the users who are responsible, accountable, consulted, and informed for each resource.
- Accounts — Files related to the Master and Model configurations; they correlate user accounts defined on endpoints with users in the configuration.

You can define other configuration files that contain subsets of Master and Model data, or newly imported data. Other files associated with a universe can include the following:

- (Optional) Approved Audit Card — A file that defines pre-approved business rule violations that are ignored in the certification processes.
- Audit Settings —A file that determines audit behavior for universe configuration files.

CA GovernanceMinder Master and Model Configurations

The Master configuration represents entities and privileges as they are in reality. The Model configuration is a development space that lets you experiment with how you might want to change the entities and privileges in your deployment.

When you import data from CA IdentityMinder, the product updates the Master and the Model configuration files. Both configuration files are the same immediately after an import. When you run a certification, the information in the Model configuration is updated to reflect the changes.

When you export data from the product back into CA IdentityMinder, CA GovernanceMinder creates a DIFF file between the Master and Model configurations. This DIFF file represents all the changes sent to CA IdentityMinder during the export.

When the export to CA IdentityMinder completes, the CA GovernanceMinder Model configuration becomes the new Master configuration.

Connectors

Connectors are defined for importing and exporting user and user privileges (entities and the links between them) from corporate systems into CA GovernanceMinder.

Import connectors are used to collect the data from corporate systems. Once that data is in the product, Role Managers can modify the data based on corporate policies and regulatory compliance.

At the end of change process, the product compares the original configuration to the new configuration and creates a variance log (DIFF file). Export connectors then push the resulting configuration changes back to the corporate system.

The CA GovernanceMinder Role Model

A CA GovernanceMinder role model is the set of roles for an organization that can result from a CA GovernanceMinder analysis, and additional input from role engineers. Once a role model is finalized and approved, it can be applied to an organization's roles to maintain a role structure.

How to Prepare the CA GovernanceMinder System

To use the product to interact with endpoint systems and provide role modeling capability, configure an environment within the product that meets your needs.

Follow these steps:

1. Set permissions and security in the Portal.
2. Create a universe.
3. Configure the connections to endpoint systems.
4. Create Business Policy Rules (BPRs).

   You have created an environment that interacts with endpoint systems and provides role model capability.

Chapter 2: Defining a CA GovernanceMinder Universe

This scenario describes how to define a CA GovernanceMinder universe.

A CA GovernanceMinder universe is a view into a management workspace that enables CA GovernanceMinder administrators to manage entities such as users, roles, and resources. Entity data is stored in the CA GovernanceMinder database. A universe consists of a specific pair of Master-Model configurations. These configurations enable you to track the differences between the real-world configuration that is imported from the system (Master), and the desired configuration generated (Model).

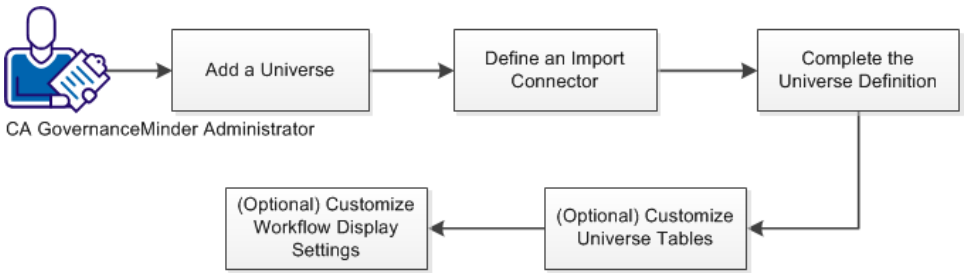
A CA GovernanceMinder universe stores imported endpoint data from such sources as CA IdentityMinder, CA IAM Connector Server, CFG, and so on.

Some of the configurations that every universe contains are as follows:

- Master - An image of the privilege model exactly as it is on the target system.
- Model - An image of the privilege model as CA GovernanceMinder prefers to be, having undergone such actions as certification, compliance, or role modeling.
- Field names (in the configuration files) that contain the following information:
  - User login credentials
  - Email address
  - User manager
  - Role manager
  - Resource manager
- Audit Settings file name.

Note: For more information about additional configurations, see the *Configuration Guide*.

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



Follow these steps:

1. Add a universe.
2. Define an import connector (see page 15).
3. Complete the Universe definition (see page 16).
4. (Optional) Customize universe tables (see page 18).
5. (Optional) Customize Workflow display settings (see page 20).

Add a Universe

To create a universe in CA GovernanceMinder, 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 GovernanceMinder 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 GovernanceMinder 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 GovernanceMinder 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 GovernanceMinder.

Follow these steps:

1. In the CA GovernanceMinder **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 GovernanceMinder.
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 GovernanceMinder 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 IdentityMinder or using the CA IAM Connector Server, ResName2 is used. Use this field to define the application during CA User Activity Reporting integration. For more information about integration between CA GovernanceMinder and CA IdentityMinder, 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 GovernanceMinder 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 GovernanceMinder **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 19) 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.

Chapter 3: Connecting to Endpoint Systems

This section contains the following topics:

Import and Export Connectors

Connectors are defined for importing and exporting user and user privileges (entities and the links between them) from endpoint systems into CA GovernanceMinder.

The CA GovernanceMinder Portal enables you to define the following import or export connectors:

Import Connectors

Custom Executable

Allows you to write a script or executable in any language (Perl, C++, C#, Java, and so on) for importing data into the product.

The executable must create three required CSV files: Users.udb, Resources.rdb, Roles.csv. The following CSV files are optional: UserRole.csv, UserRoleFields.csv, UserResource.csv, UserResourceFields.csv, RoleRole.csv, RoleRoleFields.csv, RoleResource.csv, and RoleResourceFields.csv. CA GovernanceMinder imports information from these files.

CA GovernanceMinder Configuration Document (CFG)

Reads a CA GovernanceMinder file that represents a snapshot of privileges and role definitions.

Note: CFG files created on a Windows machine cannot be imported on a Linux machine.

Generic Feed (CSV)

Reads CSV files as input, then creates a CA GovernanceMinder configuration. The CSV (Comma Separated Values) format is the most common import and export format for spreadsheets and databases. CSV files can then be manipulated and extended using simple tools such as Excel, if necessary.

The Generic Feed uses 11 CSV files as input. The following three CSV files are required: Users.udb, Resources.rdb, Roles.csv. The following CSV files are optional: UserRole.csv, UserRoleFields.csv, UserResource.csv, UserResourceFields.csv, RoleRole.csv, RoleRoleFields.csv, RoleResource.csv, and RoleResourceFields.csv. CA GovernanceMinder imports information from these files.

Database Configuration

Allows for importing information from a CA GovernanceMinder configuration (in the database) into the master and model configurations.

CA IdentityMinder

Integrates CA GovernanceMinder with CA IdentityMinder. Use the connector to import CA IdentityMinder data into CA GovernanceMinder.

Note: For more information about the CA IdentityMinder connector, see the *CA IdentityMinder Integration Guide*.

CA IAM Connector Server

Integrates the product with the CA IAM Connector Server. Use the connector to import data from a single endpoint system into the product.

Pentaho Data Integration (PDI)

Invokes Pentaho Data Integration (PDI) transformations and jobs. This feature allows for complex ETL (Extract, Transform, and Load) operations during data import. To use the PDI connector, go to Administration, System Checkup, PDI Checkup and set the PDI Home Directory.

CA ControlMinder (Shared Accounts)

Imports user-account information from CA ControlMinder using the CA ControlMinder reports database credentials.

Note: Only supports a single universe.

CA GovernanceMinder Client Batch (SBT)

Executes batch processing. You may need to specify dynamic parameters for file names that are defined in the SBT files.

Note: Running the CA GovernanceMinder Client Batch (SBT) connector from the Portal is not supported on AIX and Linux. Also, CFG files created on a Windows machine cannot be imported to a Linux machine.

Export Connectors

Custom Executable

Allows you to write a script or executable in any language (Perl, C++, C#, Java, and so on) for exporting data from CA GovernanceMinder.

The executable must create a DIFF file in the CA GovernanceMinder DIFF file format, and the product reads the DIFF file and applies the changes.

Database Configuration

Allows for exporting information from one CA GovernanceMinder model configuration to another configuration in the database.

CA IdentityMinder

Integrates CA GovernanceMinder with CA IdentityMinder. Use the connector to export updated data from the product to CA IdentityMinder.

CA IAM Connector Server

Integrates CA GovernanceMinder with the CA IAM Connector Server. Use the connector to export data to a single endpoint system.

Some user and user privileges must be imported directly into CA GovernanceMinder using the Import option in the CA GovernanceMinder Client Tools. The Import option enables importing from the following endpoints:

- Import
  - CSV files
  - LDIF files
  - Active Directory
  - RACF
  - TSS
  - UNIX
  - SAP
  - Windows Shared Folder
  - ITIM
  - Control SA
- Export:
  - Active Directory
  - RACF
  - SQL Database
  - CSV files

- ITIM V4.5 and V4.6
- Control SA

Note: For more information, see the *Client Tools Guide*.

Important! Some connectors exist in both the CA GovernanceMinder Portal and the CA GovernanceMinder Data Management client tool. In these cases, we recommend running the connector located in the CA GovernanceMinder Portal for the following reasons:

- The connector job is saved on the Portal, letting you repeat import and export tasks.
- Retrieved data is integrated directly into the universe.
- New data can be automatically synchronized with RACI definitions of the configuration.
- New user records can be automatically enriched with data from Human Resources records or other sources.

Import Data from Multiple Endpoints

A CA GovernanceMinder universe can contain any mix of the following types of endpoints.

- Managed Endpoints: Endpoints are managed by CA IdentityMinder and connected to the product.
- Discovered Endpoints: Endpoints are connected to the product using the CA IAM Connector Server.
- Unmanaged Endpoints: Endpoints whose information is imported into the product by 3rd-party utilities, such as scripts, PDI transformations, and so on.

Importing information into a CA GovernanceMinder universe from any mix of two or more types of endpoints is referred to as mixed mode (see page 27). A mixed universe can only support the shallow use case (see page 29).

Note: To create a working mixed universe, all import sources must comply with common standards. For more information about how to build a CA GovernanceMinder configuration for mixed mode, see the *CA GovernanceMinder Programming Guide*.

Merge Types

When importing data from multiple endpoint systems, consider the following *merge types* of import connectors in CA GovernanceMinder:

As Users

Connects to an endpoint system that contains users and accounts that are already correlated. Users from this endpoint are treated as users only.

As Accounts

Connects to an endpoint where users are treated as accounts. All the endpoint sub-connectors of a CA IdentityMinder connector are treated as Secondary connectors.

As Users and As Accounts

Connects to an endpoint where users are treated as users *and* as accounts. This connector type is used with the CA IAM Connector Server, so that the CA IAM Connector Server is the source for CA GovernanceMinder users and the product can also still see its accounts.

Note: You cannot change the type of a connector once it has been run.

When running an multi-import connector job, if the As Users connector fails, the entire job will fail. If the As Users connector succeeds at least once, an As Accounts connector can fail and the product uses the last successful import data from that As Accounts connector to process the multi-import job. If any connector fails in the multi-import job, the owner of the connector will get an email about the failure.

Mixed Mode Considerations

When *importing* information into a CA GovernanceMinder universe from any mix of two or more types of endpoints, consider the following:

- Import users from only one endpoint as the CA GovernanceMinder users. If CA IdentityMinder exists in your mixed universe, use the CA IdentityMinder corporate user list as the CA GovernanceMinder users.
- In CA GovernanceMinder, correlation (see page 54) determines what account belongs to what user automatically during data import. An administrator can define the set of rules that govern how CA GovernanceMinder makes decisions regarding account and user synchronization during import.
- When importing from unmanaged endpoints using CSV, Kettle, or a custom connector, the data must conform to the same standards. For more information about CSV file formats, see the *Programming Guide*.

When *exporting* information into a CA GovernanceMinder universe from any mix of two or more types of endpoints, consider the following:

- If you include CA IdentityMinder in a mixed universe, CA GovernanceMinder can only export changes to CA IdentityMinder.
- If you have a CA IAM Connector Server in a mixed universe, CA GovernanceMinder can only export changes to an endpoint if there is only that one endpoint connected to the CA IAM Connector Server. Changes to other endpoints must be processed manually.
- If you have CA IdentityMinder in your deployment, it remains synchronized with the CA GovernanceMinder Master configuration through continuous updates. With other endpoint systems or the CA IAM Connector Server, you perform another import to update the CA GovernanceMinder Master configuration.

Deep and Shallow Use Cases

CA GovernanceMinder supports two modeling strategies. You can use one of these strategies in any given CA GovernanceMinder universe.

Shallow use case

A shallow use case involves role modeling based on business or organizational roles. The shallow use case enables you to analyze roles arising from the activities of your organization, and requires the product to import data from several different endpoints. We refer to this approach as “shallow” because the use case examines data from across your organization’s endpoints to a depth of one level of application privileges. For example, this use case can analyze privileges to resources in an ERP application, Active Directory, and several Unix servers.

Deep use case

A deep use case involves role modeling based on application roles. This strategy enables you to build your role model around user permissions within a single application. For example, you would use a deep use case to analyze permissions within your organization’s SAP system. This requires the product to import data from only one endpoint. We refer to this approach as "deep" because it views the data from a granular perspective.

Note: The deep use case is supported with the CA IAM Connector Server.

Shallow Use Case

A shallow use case works with data from several different endpoints to analyze organizational roles and perform certification or role modeling. The object mapping between CA GovernanceMinder and the endpoint system is less granular than in a deep use case.

Shallow Use Case with CA GovernanceMinder and CA IdentityMinder

When importing data in a shallow use case where endpoints are managed with CA IdentityMinder, a specific universe is generated. Endpoint privileges, groups, and roles are mapped to CA GovernanceMinder resources, and CA IdentityMinder provisioning roles and account templates are mapped to CA GovernanceMinder roles. When CA GovernanceMinder exports universe data back to CA IdentityMinder, it updates changes to provisioning roles and account templates, and any additional or removed links between users, provisioning roles, nested provisioning roles, account templates, and endpoint privileges. CA IdentityMinder translates these changes into links between user accounts and endpoint privileges, and where an account does not exist, a new account is created.

CA GovernanceMinder does not export changes or additions to user attributes or resource attributes (you should manage these attributes with the user management tool or the native utilities of the endpoint, respectively).

Shallow Use Case with CA GovernanceMinder and CA IAM Connector Server

You use CA GovernanceMinder with the CA IAM Connector Server (an optional part of the CA GovernanceMinder installation) to perform shallow mapping when your endpoints are not managed with CA IdentityMinder. You do this by importing data from multiple endpoints through the CA IAM Connector Server. The selected endpoint permissions are modeled as resources, and business roles are modeled as roles. Export is not supported in this scenario.

Deep Use Case

A deep use case works with data from a single endpoint to perform certification or role modeling. The object mapping between CA GovernanceMinder and the CA IAM Connector Server is more granular than in a shallow use case. When you import data in a deep use case, you map some endpoint objects to CA GovernanceMinder resources and map other endpoint objects to CA GovernanceMinder roles. When you import data into a deep universe, ensure that you map all mandatory attributes of the endpoint to appropriate CA GovernanceMinder roles or resources.

You can use the CA IAM Connector Server to create a deep use case where you can analyze roles within an application. The CA IAM Connector Server allows you to connect to and manage endpoints in environments that are not managed by <imgr>. The CA IAM Connector Server is an optional part of the CA GovernanceMinder installation.

CA IAM Connector Server Connectivity Use Cases

Consider the following connectivity use cases when using the CA IAM Connector Server.

Note: For more information about configuring endpoints in the CA IAM Connector Server, see the *CA IAM Connector Server Online Help*.

Unmanaged Endpoints

Goal

You do *not* have an existing CA IdentityMinder12.5 SP8 (or later) deployment. You want to implement CA GovernanceMinder to perform certification on the privileges across the organization.

Environment Description

You have an Active Directory server, two UNIX servers, three Oracle databases, and a RACF managed Mainframe. You do not have CA IdentityMinder installed.

Process

1. Install CA GovernanceMinder.
2. In the CA GovernanceMinder Portal, go to Administration, Connector Server Management.

3. Create all seven endpoints in the CA IAM Connector Server.

   Note: When defining the RACF connector, you are using the CA GovernanceMinder-specific RACF connector and not the one included with CA IdentityMinder.

4. In the universe, go to the Connectivity tab and define multiple endpoint connectors.

   These connectors are run simultaneously in a multi-import job.

   Define all connectors by selecting the CA IAM Connector Server and, in each connector, select the correct endpoint. During this process, select the Active Directory server as the primary (As Users) connector.

5. Run an import.

   All data is imported through the CA IAM Connector Server. The selected endpoint permissions are modeled as resources, and business roles on the endpoint are modeled as roles.

Note the following:

- Export is not supported in this scenario.
- CA GovernanceMinder correlation is invoked on accounts of all endpoints except Active Directory. The Active Directory users appear as CA GovernanceMinder users, whereas the users of other endpoints appear as CA GovernanceMinder accounts.

Mixed Universe

Goal

You have a newly installed CA IdentityMinder 12.5 SP8 (or later) deployment with only a limited number of endpoints managed through CA IdentityMinder. You want to implement CA GovernanceMinder to perform certification on the privileges across the organization and use your new CA IAM Connector Server connectors.

Environment Description

You have an Active Directory server, two UNIX servers, three Oracle databases, and a RACF managed Mainframe. You have a newly installed CA IdentityMinder system, in which only one UNIX server and two Oracle databases are defined and managed. Now, you want to perform certifications on the privileges across the organization.

Process

1. Install CA GovernanceMinder.
2. Go to Administration, Connector Server Management and create the Active Directory endpoint, the RACF endpoint, and the unmanaged UNIX and Oracle endpoints.

   Note: When defining the RACF connector, you are using the CA GovernanceMinder-specific RACF connector and not the one included with CA IdentityMinder.
3. In the universe, under the Connectivity tab, define a connector to CA IdentityMinder. Within it, select the managed UNIX and Oracle endpoints. Select the CA IdentityMinder Connector as the primary (As Users) connector.
4. Define connectors for the unmanaged endpoints (the ones you created in Step 2) by selecting the CA IAM Connector Server and, in each connector, select the correct endpoint.
5. Run a multi-import job by selecting all the connectors.

   All unmanaged endpoint data is imported through the CA IAM Connector Server. All managed endpoint data is imported using the CA IdentityMinder connectors. The selected endpoint permissions are modeled as resources and the provisioning roles and account templates are mapped to roles.

Note the following:

- Export is supported in this scenario only for the endpoints managed by CA IdentityMinder. The other endpoints must be provisioned manually.
- CA GovernanceMinder correlation is invoked on unmanaged endpoint accounts. The CA IdentityMinder users appear as CA GovernanceMinder users, whereas all endpoint users appear as CA GovernanceMinder accounts.

Mixed Universe with Custom Endpoints - Example 1

Goal

You have a newly installed CA IdentityMinder 12.5 SP8 (or later) deployment with only a limited number of endpoints managed through the CA IAM Connector Server. You also have a number of custom or third-party systems that support an LDAP or JDBC connection. You want to implement CA GovernanceMinder to perform certification on the privileges across the organization and use your new CA IAM Connector Server connectors.

Environment Description

You have an Active Directory server, two UNIX servers, three Oracle databases, and two custom systems that use an LDAP or SQL interface. You have a newly installed CA IdentityMinder deployment, in which only one UNIX server and two Oracle databases are already defined and managed. It is assumed that the implementation team has developed dynamic connectors for the custom or third-party systems, using Connector Xpress.

Note: When developing the dynamic connector using Connector Xpress, each attribute has a new flag named Interesting for Compliance. The attributes with this flag represent privileges that must be certified in CA GovernanceMinder. For more information, see the Extended Metadata Properties section of the *Connector Xpress Guide*.

Process

1. Install CA GovernanceMinder.
2. After the new dynamic connector is ready, use Connector Xpress to push its definition to the CA IAM Connector Server installed with CA GovernanceMinder.
3. In the CA GovernanceMinder Portal, go to Administration, Connector Server Management.
4. Define the Active Directory server and the unmanaged UNIX and Oracle endpoints in the CA IAM Connector Server.
5. In the universe, go to the Connectivity tab.
6. Define a connector to CA IdentityMinder. Select the managed UNIX and Oracle endpoints and set this connector as the primary (As Users) connector.

7. Define connectors for the unmanaged endpoints, including the dynamic connector, by choosing the CA IAM Connector Server and, in each connector, choosing the correct endpoint.
8. Run all the import connectors at once through a multi-import job.

   All unmanaged endpoint data, including the dynamic connector data, is imported through the CA IAM Connector Server connectors. All managed endpoint data is imported through the CA IdentityMinder connectors. The selected endpoint permissions are modeled as resources and the provisioning roles and account templates are mapped to roles.

Note the following:

- Export is supported in this scenario only for the endpoints managed by CA IdentityMinder. The other endpoints must be provisioned manually.
- CA GovernanceMinder correlation is invoked on unmanaged endpoint accounts. The CA IdentityMinder users appear as CA GovernanceMinder users, whereas all endpoint users appear as CA GovernanceMinder accounts.

Mixed Universe with Custom Endpoints - Example 2

Goal

You have a newly installed CA IdentityMinder 12.5 SP8 (or later) deployment with only a limited number of endpoints managed through the CA IAM Connector Server. You also have a number of custom or third-party systems that are accessed through Pentaho Data Integration (PDI). You want to implement CA GovernanceMinder to perform certification on the privileges across the organization and use your new CA IAM Connector Server connectors.

Environment Description

You have an Active Directory server, two UNIX servers, three Oracle databases, and two custom systems that expose proprietary interfaces (not LDAP or SQL). You have a newly installed CA IdentityMinder deployment, in which only one UNIX server and two Oracle databases are already defined and managed. It is assumed that the implementation team has developed PDI transformations for the custom applications using Pentaho Kettle.

Process

1. Install CA GovernanceMinder.
2. In the CA GovernanceMinder Portal, go to Administration, Connector Server Management.
3. Define the Active Directory server and the unmanaged UNIX and Oracle endpoints in the CA IAM Connector Server.

4. In the universe, go to the Connectivity tab.
5. Define a connector to CA IdentityMinder. Select the managed UNIX and Oracle endpoints and set this connector as the primary (As Users) connector.
6. Define connectors for the unmanaged endpoints, including the dynamic connector, by choosing the CA IAM Connector Server and, in each connector, choosing the correct endpoint.
7. Define two connectors for the custom systems by selecting the PDI connector. Fill in the appropriate parameters for this connector.
8. Run all the import connectors at once through a multi-import job.

   All unmanaged endpoint data, including the dynamic connector data, is imported through the CA IAM Connector Server connectors. All managed endpoint data is imported through the CA IdentityMinder connectors. All custom system data is imported by executing the provided solution.

   The selected endpoint permissions are modeled as resources and the provisioning roles and account templates are mapped to roles.

Note the following:

- Export is supported in this scenario only for the endpoints managed by CA IdentityMinder. The other endpoints must be provisioned manually.
- CA GovernanceMinder correlation is invoked on unmanaged endpoint accounts. The CA IdentityMinder users appear as CA GovernanceMinder users, whereas all endpoint users appear as CA GovernanceMinder accounts.

Deep Analysis of an Endpoint - Example 1

Goals

You want to implement CA GovernanceMinder to perform privilege cleanup and role mining over your data.

Environment Description

You have a number of custom or third-party systems that support an LDAP or JDBC connection. It is assumed that the implementation team has developed dynamic connectors for the custom or third-party systems using Connector Xpress.

Note: When developing the dynamic connector using Connector Xpress, each attribute has a new flag named Interesting for Compliance. The attributes with this flag represent privileges that must be certified in CA GovernanceMinder. For more information, see the Extended Metadata Properties section of the *Connector Xpress Guide*.

Process

1. Install CA GovernanceMinder.
2. After the new dynamic connector is ready, use Connector Xpress to push its definition to the CA IAM Connector Server installed with CA GovernanceMinder.
3. In the CA GovernanceMinder Portal, go to Administration, Connector Server Management.
4. Define the SAP endpoint in the CA IAM Connector Server.
5. In the universe, go to the Connectivity tab.
6. Define a connector. Select the CA GovernanceMinder CA IAM Connector Server and specify the dynamic endpoint. Within it, map some endpoint objects (that you defined with the "Interesting for Compliance" flag) to CA GovernanceMinder roles and others to CA GovernanceMinder resources.
7. Run an import. All data is imported through the CA IAM Connector Server connector.

   The resources and roles appear as mapped.

Note the following:

- Export is supported in this scenario.
- Correlation is irrelevant in this scenario, as it only works with one system.

Deep Analysis of an Endpoint - Example 2

Goals

You want to implement CA GovernanceMinder to perform privilege cleanup and role mining over your Mainframe data.

Environment Description

You have a RACF Managed Mainframe.

Process

1. Install CA GovernanceMinder.
2. In the Portal, go to Administration, Connector Server Management.
3. Define the RACF endpoint in the CA IAM Connector Server. In this scenario, you use the CA GovernanceMinder-specific RACF connector and not the one included with CA IdentityMinder.
4. In the universe, go to the Connectivity tab.

5. Define a connector. Select the CA GovernanceMinder CA IAM Connector Server and specify the RACF endpoint. Within it, map RACF groups to CA GovernanceMinder roles and map data sources as CA GovernanceMinder resources.
6. Run an import. All data is imported through the CA IAM Connector Server connector.

   The resources and roles appear as mapped.

Note the following:

- Export is not supported in this scenario, as there is no support by the connector.
- Correlation is irrelevant in this scenario, as it only works with one system.

Mixed Universe with Role Modeling

Goal

You have an existing CA IdentityMinder 12.5 SP8 (or later) deployment with a significant number of endpoints managed through the CA IAM Connector Server. You want to implement CA GovernanceMinder to perform certification on the privileges across the organization using the CA IAM Connector Server connectors, and also perform privilege cleanup and role modeling.

Environment Description

You have an Active Directory server, two UNIX servers, three Oracle databases, and a RACF managed Mainframe. You have an existing CA IdentityMinder deployment where all seven endpoints are defined and managed.

Note: This scenario is unique, as CA GovernanceMinder interfaces with RACF in two different ways, using two different connectors. When retrieving CA IdentityMinder data, the native CA IdentityMinder RACF connector is used, but when working with CA GovernanceMinder, the CA GovernanceMinder-specific CA IAM Connector Server connector is used.

Process

1. Install CA GovernanceMinder.
2. In CA GovernanceMinder, create two universes, for example, "Org" and "RACF".

3. In the universe "Org", perform the following steps:
   a. Go to the Connectivity tab and define a connector to CA IdentityMinder.
   b. After providing CA IdentityMinder connection details, select all endpoints or use the "all" wildcard.
   c. Run the import.

      All data is imported through CA IdentityMinder connectors. The selected endpoint permissions are modeled as resources, and provisioning roles and account templates are modeled as roles.
4. For the universe "RACF", perform the following steps:
   a. In the CA GovernanceMinder portal, go to Administration, Connector Server Management.
   b. Define the Top Secret endpoint in the CA IAM Connector Server. In this scenario, you are using the CA GovernanceMinder-specific Top Secret connector and not the one included with CA IdentityMinder.
   c. In the universe, go to the Connectivity tab.
   d. Define a connector. Select the CA GovernanceMinder CA IAM Connector Server and specify the Top Secret endpoint. Within it, map Top Secret groups to CA GovernanceMinder roles and map data sources as CA GovernanceMinder resources.
   e. Run the import.

      All data is imported through the CA IAM Connector Server connector that is specific for CA GovernanceMinder. The resources and roles appear as mapped.

Note the following:

- Export is fully supported in the "Org" universe. Export is not supported in the "RACF" universe, as there is no support by the connector.
- CA GovernanceMinder correlation is not invoked. In the "Org" universe, CA IdentityMinder is relied on to provide the associations between users and accounts, whereas in the "RACF" universe, correlation is not relevant because it contains only one source.

Define an Import Connector

CA GovernanceMinder import connectors import data from endpoint systems.

Follow these steps:

1. Login to the CA GovernanceMinder Portal as an administrator.
2. Go to Administration, Universes.

   A list of universes appears.

3. Click on the universe you want to import data to.
4. Select the Connectivity Tab.

   The Connector screen opens.
5. Be sure that the Import option button is selected and click Add Connector.

   The Connector wizard appears.
6. Provide values for all mandatory connector settings.

   Note: For the CA IdentityMinder connector (see page 51) and the CA IAM Connector Server connector, additional steps are necessary.
7. Click Finish.

   The new import connector is defined in CA GovernanceMinder.
8. (Optional) Once the connector is saved, you return to the import connector screen. You can now edit the merge type (see page 27) of the connector you just defined under the Merge Type column.
9. (Optional) Click the Owner link next to the new connector and set a user as the owner of the connector. This user is notified by email if the connector fails during an import or export job.
10. (Optional) Select the new connector and click Validate.

    The connector parameters and configuration are validated.

Note: A matching export connector is automatically defined in CA GovernanceMinder for every import connector you define.

Import Flow Properties

The following options are available when running import connectors:

Synchronize permissions and RACI configurations

The CA GovernanceMinder Server uses RACI configurations to control end-user access to the CA GovernanceMinder Portal. When you import new user records into a configuration, you can automatically enroll these new users in that RACI configuration hierarchy.

Note: If an imported user does not have a login name (LoginID field is blank), they cannot access the CA GovernanceMinder Portal. The RACI synchronization process flags these users, and notifies the Portal administrator.

Remove redundant links

Deletes redundant links that are direct relationships between users and resources that exist in addition to indirect relationships, such as through a role. You may prefer to remove redundant links during import, so that user access to a resource depends on continued membership in a role.

Run audit

Performs the auditing process on the imported configuration to locate erroneous privileges and other deviations from policies.

Set PDI Transformation on merged data

Runs a PDI transformation on imported data that has been merged into a single configuration. For example, if you want to know how many accounts a user has, you can run a PDI transformation on merged data to calculate the number.

Purge temporary audit cards and configurations

Deletes the import configuration and the audit card that outlines differences between the import configuration and the Master configuration. Purging the information saves space on your system.

Delete last successful import data for each connector

Deletes that last successful import configuration. Purging the information saves space on your system.

Filter Imported Data

When defining an import connector to CA IdentityMinder or the CA IAM Connector Server, you can specify the objects you want to import into a universe. This filter can be useful when you want to separate data into different universes, or ignore data for performance reasons.

All import filters use the LDAP filter format and support 'AND' type queries only. You can filter on the following: Corporate Users, Provisioning Roles, Account Templates, and Accounts.

Using the CA IAM Connector Server

The CA IAM Connector Server allows you to connect to and manage endpoints without CA IdentityMinder in your environment. CA GovernanceMinder uses the CA IAM Connector Server to automatically import and export data from a single endpoint.

Installing the CA IAM Connector Server is an option in the CA GovernanceMinder installer.

To access the CA IAM Connector Server after installation, go to Administration, Connector Server Manager in the Portal.

Note: For more information about configuring endpoints in the CA IAM Connector Server, see the *CA IAM Connector Server Online Help*.

Define an Import Connector to the CA IAM Connector Server

To define an import connector to the CA IAM Connector Server, use the import connector wizard under the connectivity tab of the universe. The wizard guides you through mapping users, roles, and accounts to CA GovernanceMinder.

The following steps are reflected in the connector wizard. Perform these steps to define a connector to the CA IAM Connector Server.

1. (Connection Settings) Provide the connection information to the CA IAM Connector Server.

   Note: The Login Name must be a full DN.

2. (Endpoint) Select the endpoint type and endpoint to connect to.

3. (Endpoint Configuration) Under Endpoint Template, select one of the following options:

   Note: For more information about endpoints, and endpoint objects and attributes, see the Endpoint Guides on CA Support.

   - (Recommended) Use template—loads a default template for the endpoint, mapping endpoint objects to appropriate CA GovernanceMinder resources or roles.
   - Use template from file—allows you to browse and load an existing endpoint template from a file.

     Note: If you want to adjust the endpoint mappings of a loaded template, select the Fine tune the selected endpoint template check box.

   - Use custom configuration (see page 42)—allows you to create your endpoint configuration manually.

     Important! Custom configuration of an endpoint requires advanced knowledge of the endpoint and CA GovernanceMinder, and how each system treats objects. Use the default template if you are not familiar with these concepts.

4. (Optional Enrichment) Provide the supplementary enrichment file and matching information.

   During an import, you can merge supplementary user or resource data with the imported data.

5. Summary

   Review the connector information and click Finish to save the connector.

6. (Optional) Once the connector is saved, you return to the import connector screen. You can now edit the merge type (see page 27) of the connector you defined under the Merge Type column.

Define a Custom Configuration for the Endpoint

Important! For more information about endpoints, and endpoint objects and attributes, see the Endpoint Guides on CA Support.

If you select Use custom configuration for your endpoint template, manually provide mappings between the CA IAM Connector Server endpoints and CA GovernanceMinder.

Note: Avoid changing attribute mappings in connector configurations once you have run an initial import. If you do change the mapped attributes after initial import, it could cause significant performance impact.

1. Under Define User Accounts, map endpoint account attributes to CA GovernanceMinder account attributes.

   Note the following:

   - Use the filter to import a subset of accounts from the CA IAM Connector Server.
   - Click Add in the right-hand corner of the User Mapping section to add more user mappings between CA GovernanceMinder and the CA IAM Connector Server.

2. Click Next.
3. Define associations for the endpoint. This screen allows you to do the following:

   - Define how objects in an endpoint map to objects in CA GovernanceMinder, for example, a group in Active Directory is a resource in CA GovernanceMinder
   - Define how different objects are linked
   - Define additional properties for both objects and links, where available

   Define associations as follows:

   a. (Optional) If you want set up mappings for a deep use case (see page 30), select the Enable deep use case associations check box.

      Note: When importing data into a deep universe, verify that you map all mandatory attributes of the endpoint to appropriate CA GovernanceMinder roles or resources.

   b. Under Association List, click Add to the right.

   c. Select the initial object type (specific to the endpoint) to associate in the From object type drop-down list.

   d. Select the relationship attribute used to associate the two objects.

e. Click Ok.

f. (Optional) Under Custom association fields mapping, click Add to provide any custom association attribute mapping information.

Some associations have additional data related to them stored in attributes. Add the attribute mapping information if there is an attribute related to the association.

Click Ok.

4. At this point, the associated objects do not yet relate to a known CA GovernanceMinder resource or role. Define the relation to a resource or role as follows:

a. If the initial object type is not an account, select a CA GovernanceMinder role or resource to associate. Click the active link 'Select RCM role/resource' under the From "Account" or "RCM Role/Resource" column.

b. Provide a name for the CA GovernanceMinder resource or role.

c. (Optional) Click Edit to add field mappings for the related object.

You can map attributes on the endpoint object to fields on the CA GovernanceMinder resource or role.

d. Click Ok.

e. Under the To "RCM Role/Resource" column, click the active link 'Select RCM role/resource'.

f. Provide a name for the CA GovernanceMinder resource or role.

g. (Optional) Click Edit to add field mappings for the related object.

You can map attributes on the endpoint object to fields on the CA GovernanceMinder resource or role.

h. Click Ok.

5. Repeat Steps 3 and 4 for each association.

6. Click Ok.

Note: If you want a shallow (see page 29) use case, associate an account to a CA GovernanceMinder resource. For a deep (see page 30) use case, map an account to a role, map the role to a resource, and optionally, map the account to a resource.

Associations Overview

Object in CA IdentityMinder compared to objects in CA GovernanceMinder

When looking at CA GovernanceMinder and the CA IAM Connector Server and how they handle linked objects, there are some differences. Because of these differences, we must map associations between the two systems so that both CA GovernanceMinder and the CA IAM Connector Server understand the relationships between objects. In CA GovernanceMinder, two objects are linked without dealing with how they are linked. In the CA IAM Connector Server, two objects are linked through an attribute. For example, in CA GovernanceMinder, an Active Directory account and a resource that represents a group can be linked. In the CA IAM Connector Server, the account is connected to the group through an attribute named "groupMembership". Without telling the CA IAM Connector Server which attribute to use, you cannot connect the group to the account.

The Issue

When mapping associations (which become links in CA GovernanceMinder) you must reduce the definition of the link from containing three values (from what object, to what object, and through which attribute) to only two values (from which object to which object). This reduction happens during import from the CA IAM Connector Server to CA GovernanceMinder, but an issue arises when building the three-value definition out of two values when exporting back to the CA IAM Connector Server. Once you map an association, you provide both the attribute and the object name in the endpoint. When you export a link, the connector then knows which resource is linked to the account. All three values are now available for CA GovernanceMinder to export.

Once mapped, the CA GovernanceMinder resource refers to both the mapped object in (AD group) and the attribute (groupMembership). If an account can be connected to the same object by different attributes, the account must be defined as multiple resources in CA GovernanceMinder. Each resource then represents an object linked by a specific attribute. These multiple resource definitions allow the export to identify which attribute the user referred to when connecting a resource to the account.

This issue affects roles too. An endpoint object can be mapped to a role in CA GovernanceMinder, but it is still connected to the account using an attribute. Also, a resource is connected to both the account and the role, but it could be connected to each through different attributes.

Note: A resource with no association is not understood between the two systems.

Example

For example, Unix has an account connected to Unix groups using either the "primary group" attribute or the "group membership" attribute. If there is only one resource in CA GovernanceMinder named "Unix group" when it is mapped to an account, CA GovernanceMinder does not know whether to use the primary group or the group membership attribute when exporting to the CA IAM Connector Server. Therefore, you map two associations, each to a different resource. For example, if the Unix endpoint has group "A", then you map two resources, one representing "A", "primary group" and the other representing "A", "group membership". Then CA GovernanceMinder reads the associations and understands which attribute was referred to when it exports the data.

Working with Associations

After defining how endpoint objects are linked, you map them to CA GovernanceMinder objects by giving names to the CA GovernanceMinder roles and resources. Initially, an object on the endpoint is marked as a resource and CA GovernanceMinder offers to name the resource using the name of the object. After an object is mapped to a resource, if that object is used in other associations, the existing resource or role definition must be used. However, if you have more than one association between two exact objects linked by different attributes, you cannot use the same resource or role definition for both associations, and the endpoint object must be mapped to a new resource or role in CA GovernanceMinder.

Because each resource is mapped to an object on the endpoint, attributes can be mapped from the endpoint object to the resource. For example, a resource representing an AD group can have an attribute containing the group description. This option is not currently applicable to roles, as they cannot have custom attributes in CA GovernanceMinder.

Associations that do not start from an account are only possible in a deep use case. A deep use case is only available with the CA IAM Connector Server. If a deep use case is used, the mapping must have an account connected to a role and a role connected to a resource. The association between the account and the resource directly should also be defined, though not enforced.

Custom Association Attributes (Link Attributes)

An association itself can have attributes in the form of link attributes. Link attributes define that the link between two objects has a risk, so there is a risk attribute with a value. For example, you have an association between an SAP account and a role. A role is an object that can be mapped to a resource. Different accounts can have the same role. However, each account is linked to the role for a restricted time period. The association itself has attributes that contain the start and end dates for the restricted time period.

Enrichment

During an import, you can merge supplementary Human Resources (HR) or additional resource data with the existing users or resources databases. In a deep use case, you can also add supplementary role data during import.

For every field in the database that has a matching field in the enrichment file, CA GovernanceMinder updates the record in the database according to the enrichment setting in the file. This feature allows you to add data that does not exist in the endpoint that may be useful during certification. Also, extra data may be required for correlation in some cases.

A supplementary enrichment file must be in CSV file format.

When performing enrichment, select the attribute in both the database and the enrichment file that you want to use to match records. You can specify this match to be case-sensitive.

Note: An enrichment file record can match multiple database records, for example, matching the department field in the users database updates all the users in the same department.

The following options are available when performing enrichment during an import:

(Users and Resources only) Update fields that are different from enrichment file

Select this option to change the fields in the database if they differ from the enrichment file. Clear the option to keep the data in the database and add any deltas from the enrichment file.

Clear Fields that are empty in the enrichment file

Select this option to delete data for a field if the corresponding entry in the enrichment file is blank. Clear the option to disregard empty fields in the enrichment file and keep the existing content in the database.

Resolve Manager IDs for Certification

In some cases, attributes reference a user, but the value of the attribute is not the same as the person ID. For example, the "manager" field in Active Directory contains a DN to the manager. If you bring the DN value of the "manager" field into CA GovernanceMinder, the system cannot identify who the manager is.

To address this issue, you can map a lookup attribute to the Manager ID (or Owner) field in CA GovernanceMinder. The lookup attribute is the attribute of the manager, where the default is Person ID. In the previous Active Directory example, the manager has an additional DN attribute, and the lookup attribute for the user must be set to DN to reflect that when looking for the manager, CA GovernanceMinder must search for a user with the value in the DN field that equals the value in the "Manager ID" field.

This attribute replacement occurs during the import process, so the RACI and user permissions see the replaced value.

Note: Map the lookup attribute to the Manager ID field for the endpoint type of 'As Users (see page 27)'.

Example

Consider the following two users:

User 1

- Person ID: Steve
- Manager ID: 54371 (endpoint value)
- ID Number: 79882

User 2

- Person ID: John
- Manager ID: 43582 (endpoint value)
- ID Number: 54371

In this example, there is no attribute on the user 'Steve' that contains the Person ID of his manager, so CA GovernanceMinder cannot recognize John as the manager. This issue prevents you from doing a certification, as CA GovernanceMinder needs the value of the Manager ID to say "John". The lookup attribute does a search and replaces the value. If you entered a lookup attribute of "ID Number", CA GovernanceMinder searches for a user with an ID Number that matches the Manager ID attribute for Steve, which results in "John". CA GovernanceMinder then takes that Person ID (John) and writes it to the Manager ID attribute, instead of the current value (54371).

Because this replacement happens on import, CA GovernanceMinder sets the Manager ID field to "John" instead of 54371. CA GovernanceMinder behaves as if "John" was the value all along, so everything else in CA GovernanceMinder including RACI, permissions, and certifications only see the new value.

Note: The field to set the lookup attribute is located at the bottom of the Default User Accounts screen when creating a CA IAM Connector Server connector, and it is labeled "Lookup attribute for 'Manager ID'/'Owner' search".

Map Person ID to Ensure Unique User IDs

If you have an endpoint with a display name that is not unique, map the Person ID field to another attribute. For example, you have the following two accounts on Active Directory with the same display name:

- smijo09 - John Smith
- jsmith - John Smith

In this scenario, the account display name is "John Smith" for both accounts, and "John Smith" is sent to CA GovernanceMinder as the unique user ID for both accounts. This scenario creates a problem in CA GovernanceMinder as the display name for both accounts is not unique.

To fix this issue, map the Person ID field to another attribute in the endpoint. For Active Directory, map the Person ID field to the ntAccountID (Account ID before Microsoft Windows 2000) attribute. This mapping would send 'smijo09' and 'jsmith' as the unique user IDs for the accounts in the previous example.

Hide the Custom Configuration Option in the Connector Wizard

If you do not want to allow users to customize endpoint mappings when defining a connector to CA IdentityMinder or the CA IAM Connector Server, you can hide the 'Use custom configuration' option in CA GovernanceMinder. The following property controls whether a user can access the custom configuration option when defining a connector to CA IdentityMinder or the CA IAM Connector Server.

universe.property.*universe_name*.endpointAssociations.enabled

Defines whether the custom configuration option appears in the connector wizard. When true, the option to customize endpoint mappings appears. When false, the option to customize endpoint mappings is not available. Also, when set to false, the user cannot configure associations for loaded endpoint templates.

Default: True

How to Import Data from Dynamic Connectors

When using Connector Xpress, perform the following these steps to import data from a dynamic connector to CA GovernanceMinder.

1. In Connector Xpress, define a dynamic connector.

   Be sure to select the 'Is Interesting to Compliance' check box for any attribute that you want to be interesting to CA GovernanceMinder. For example, an attribute of an account marked as interesting to compliance is available to CA GovernanceMinder as a resource for analysis. Typically these attributes signify the assignment of a permission or entitlement on the endpoint system.

   Note: For more information, see the *Connector Xpress Guide*.

2. Deploy the dynamic connector to the CA IAM Connector Server on the CA GovernanceMinder server.

3. In the CA GovernanceMinder portal, create a CA IAM Connector Server connector to import data from the endpoint.

   When you create this connector, you define the attribute mappings between endpoint objects and CA GovernanceMinder roles and resources.

Note: There are two ports (non-TLS/SSL and SSL) that a client can use to communicate with the CA IAM Connector Server. To allow Connector Xpress to access the CA IAM Connector Server, configure the firewall on your CA IAM Connector Server server host to allow communication on these ports.

Turn on Connector Server Logging

You can turn on CA IAM Connector Server endpoint specific logging and set the log4j severity level.

Follow these steps:

1. Open the *jcs-home* \conf\log4j.properties file.
2. Change the log4j severity level in the following line:

   ```
   log4j.category.jcs_conn=OFF, jcs_conn_Appender
   ```

   For example, log4j.category.jcs_conn=DEBUG, jcs_conn_Appender changes the severity level to debug.

   Note: For more information about log4j severity levels, see Logging Severities in the *CA IdentityMinder Java Connector Server Implementation Guide*.
3. Restart the CA IAM Connector Server.

C++ Connector Server Trace Logging

C++ Connector Server Trace Logs record the activity of the C++ Connector Server, which is a module used to help manage many endpoint types. This log performs the following functions:

- Logs trace and debug messages for the C++ Connector Server.
- Monitors all statuses returned by its connectors. For example, if a connector returns fatal LDAP errors, the C++ Connector Server logs these errors with severity LOG_FATAL.

To set the log file name and logging levels in im_ccs.conf set the SATransLog and SATransLogLevel parameters. The supported logging levels are 0 (for off) and 1 (for on). The default is 0. These parameters must exist in the file after the database superagent line.

CA IAM Connector Server Using Domain Other Than 'IM'

Symptom:

I deployed the CA IAM Connector Server and provided a domain name other than 'im' during the installation. When I try to import data into CA GovernanceMinder, the import fails.

Solution:

If you want to use a domain other than 'im', change the following setting in the server_jcs.xml file on the CA IAM Connector Server system, then restarts the CA IAM Connector Server:

```
<!-- Standalone Connector Server -->
  <bean id="standaloneConfiguration"
class="com.ca.jcs.standalone.StandaloneServerConfiguration">
    <property name="enabled" value="true" />
    <property name="baseDn" value="dc=etasa" />
    <property name="domain" value="im" />
    <property name="configContainer" value="eTConfigContainerName=SA
Configuration,dc=etasa" />
  </bean>
```

Connect to CA IdentityMinder

To get CA IdentityMinder data to CA GovernanceMinder, you perform an import. The import process updates both the Master and Model configurations in CA GovernanceMinder and populates a specific universe.

A CA GovernanceMinder universe is coupled with an CA IdentityMinder Environment, and you import Identity Manager users as the CA GovernanceMinder users. Endpoint objects are imported as CA GovernanceMinder resources only.

You can customize the following data you want to import:

- What types of endpoint objects to import. If you only want a subset of a particular object type, you can also apply filters to the data that is imported.

  Note: When you use filters in defining a connector to CA IdentityMinder, the same filters are used when receiving continuous updates from CA IdentityMinder , so as to ignore notifications that do not match the filter.

- What attributes are mapped to what CA GovernanceMinder fields.

To push updated CA GovernanceMinder data to CA IdentityMinder, you perform an export. The export process takes the differences between the Master and Model configurations, creates a DIFF file and sends those changes to CA IdentityMinder. Once CA IdentityMinder completes all the changes defined in the export task, it sends a notification back to CA GovernanceMinder. At that time, CA GovernanceMinder updates the Master to reflect what is in the Model and Continuous Update keeps CA IdentityMinder and the CA GovernanceMinder Master configuration synchronized.

An export from CA GovernanceMinder now updates data in the CA IdentityMinder object store, and *not* the Provisioning Server. This allows you to take advantage of the following CA IdentityMinder features:

- CA IdentityMinder task model
- CA IdentityMinder transaction logging
- CA IdentityMinder policy triggers

Note: For more information about connecting to CA IdentityMinder, see the *Integration Guide*.

Add or Modify Data During Import

As an administrator, you may want to transform data to a format that is convenient for system users before it is loaded into CA GovernanceMinder. To transform the data during an import, run a PDI transformation during the import process.

For example, you have roles on an endpoint that you are importing to CA GovernanceMinder, but the role names are technical and do not describe the purpose of the role in any way. In order for Analysts to know what types of roles they are reviewing, you can transform the role names to something more descriptive during import.

Follow these steps:

1. Verify the PDI application on the server (see page 53).
2. Upload the PDI package to the server (see page 53).
3. Configure an import to run with a transformation. (see page 54)

Verify the PDI Application on the Server

To run PDI transformations in CA GovernanceMinder, provide the location of the PDI application on the server and verify that the directory is configured correctly.

Follow these steps:

1. (AIX or Linux only) Check that the os.commandInterpreter property is set.
   - Linux: /bin/bash
   - AIX: /usr/bin/bash
2. In the CA GovernanceMinder Portal, go to Administration, System Checkup, PDI Checkup.
3. Define the value of the PDI Home Directory.

   Note: This should be completed on every CA GovernanceMinder host.
4. Click Check.

   CA GovernanceMinder checks that the PDI application directory is configured for both a single server and a cluster deployment of CA GovernanceMinder.

Upload the PDI Package

To modify data that is imported, upload a PDI transformation package to the server.

Note: For more information on creating a PDI transformation, see the Programming Guide.

Follow these steps:

1. Add the KTR file and all additional files it uses to a ZIP file.

   Note: Package the transformation in a ZIP file even if there are no additional files.
2. Go to Administration, Workflow Settings, Manage PDI Packages.
3. Select a universe.
4. Click Add New.
5. Add the new package as follows:
   a. Provide a name and description.
   b. Click on the edit icon next to Attachment and upload the zip file.
   c. The KTR file is now available. Select it under Main File.

      Any available parameters show in the list below.
6. Click Save.

   You can now use the transformation package during an import.

Configure an Import to Run with a Transformation

If you want to add or modify data when importing data to CA GovernanceMinder from a single endpoint, run an import connector with a PDI transformation loaded onto the server.

Follow these steps:

1. In the Portal, go to Administration, Universes, *Universe*, and click the Connectivity Tab.
2. Click PDI For Selected to add a PDI transformation for the selected connectors.

   A popup appears with a list of available PDI packages.
3. Select the PDI package to use.
4. The following parameters are automatically set:
   - RCM_SERVER_URL—populated from the sage.sageBaseUrl property. To override, use the pdi.serverUrl property.
   - RCM_LOGIN_NAME—populated from the batch user (sage.batch.login). To override, use the pdi.loginUser property.
   - RCM_PASSWORD—populated from the batch user password (sage.batch.password). To override, use the pdi.loginPassword property.
   - RCM_UNIVERSE
   - RCM_CONFIGURATION

   Set any additional parameters for the transformation.
5. (Optional) Encrypt the value by selecting the Encrypt check box.

Correlate Imported Accounts to Users

CA GovernanceMinder imports accounts from endpoints. You define how CA GovernanceMinder matches these accounts to users in the universe.

Note: When you import endpoint data using CA IdentityMinder, accounts are already mapped to users. Define account mapping logic for connectors that use the CA IAMS Connector Server or connectors that import data files.

To create correlation logic, use the Correlation tab of the Universe screen. Typically you define, test, and refine the settings of this tab in several iterations to achieve the mapping behavior that you want. Define the following settings:

Correlation Rules

Correlation rules compare fields in imported accounts to known user attributes so that CA GovernanceMinder can associate accounts with existing users. A score assigned to each rule indicates how strongly the rule predicts a real user-account link. You can apply string manipulations to attribute values, so that rules match sub-strings such as the first or last name of a personID. One correlation rule can test several conditions.

You can define rules that match account fields to any user attribute. Rules that match the personID user attribute have the highest scores, indicating the most confidence in the user-account link. Rules that match other user attributes have lower scores - they do not identify a unique user, but can confirm a match.

Note: Analyze the account data to identify the string patterns used on each endpoint. For example, email accounts can use variations on the personID value, as in the following examples for user Ellen Hayek:

Ellen.Hayek@companyserver.com

EHay023@companyserver.com

Synonyms

Synonyms let one correlation rule test common string variants that may represent the same value. The synonym file defines sets of synonyms. When a string expression in a rule equals a term in the synonym file, CA GovernanceMinder tests the rule using each synonym of the term. For example, if the synonym file lists Nathaniel, Nathan, Nate, Nat as synonyms, CA GovernanceMinder tests correlation rules for a user named Nathan using each of the alternate terms.

Correlation Thresholds

Correlation thresholds determine how CA GovernanceMinder evaluates user-account pairs that match correlation rules. For each user, CA GovernanceMinder aggregates the scores of all matched rules. CA GovernanceMinder decides to accept or reject the user-account mapping by comparing the aggregate score to the thresholds.

CA GovernanceMinder applies thresholds as follows:

- If all matching users score less than the Low Threshold, no user is mapped to the account.
- CA GovernanceMinder maps the account to the first user whose aggregate score exceeds the High Threshold.

- When only one user scores between the Unique and High Thresholds, CA GovernanceMinder maps the account to this user.
- When one or more users score between the Low and High Thresholds, CA GovernanceMinder submits all matching users for review by a manager.

Aggregation Type

Defines the way rule scores are aggregated when more than one rule matches the same user-account pair. For example, you have the following two rules:

Rule A - Score 60

Rule B – Score 30

And they both match User1 to Account1. The final score of this pair is as follows, depending on which aggregation type you select:

- Sum: 90 (if the sum is more than 100, it is limited to 100)
- Max: 60
- Average: 45
- Combined Probability: Measures the probability of a user-account pair that matches a particular rule to be the correct match. If two rules point to the same match, CA GovernanceMinder uses the combined probability to calculate the new score. The example has a match of 60 and a match of 30. If we improve the 60 score by 30 percent we reach 72.

Define Account Correlation Rules

CA GovernanceMinder imports accounts from endpoints. Use the Correlation tab to define how CA GovernanceMinder matches these accounts to users in the universe. CA GovernanceMinder executes correlation rules automatically when importing account data. In addition, options on this screen let you remove account-user links and manually invoke correlation.

Note: When you import endpoint data using CA IdentityMinder, accounts are already mapped to users. Define account mapping logic for connectors that use the CA IAMS Connector Server or connectors that import data files.

To define account correlation rules

1. Define correlation rules for each endpoint as follows:
   - To define new correlation rules, click Add New Rule under Correlation Rules.
   - To base correlation logic on an existing set of rules, click Import Rules from XML. Edit the endpoint attributes and test expressions as necessary.

Define a correlation condition consisting of the following terms:

- User Expressions - one or more string expressions based on user attributes in the universe.
- Comparator - compares the result of the user expression to the result of the account expression.
- Account Expressions - one or more string expressions based on account attributes.

  (Optional) Select the Consider Synonyms option to test the condition with string variants in the synonyms file.

You can define several correlation conditions in a single rule. A user-account pair matches the rule only when it satisfies *all* the conditions.

The table under Correlation Rules lists active rules.

2. (Optional) Define sets of string variants. Under Manage Synonyms, do any of the following:
   - To load a default synonym list, click Load Synonyms Defaults.
   - To load your own custom synonym list, click Import Synonyms.
   - To add synonyms individually, click Add Synonyms.
3. Define correlation thresholds under Correlation Parameters, and specify how CA GovernanceMinder calculates the aggregated score.
4. Specify correlation reviewers under Correlation Flow Properties.

   When accounts are not immediately correlated to a user (based on the score), they are sent to one or more users for approval. The reviewer then chooses the user to correlate the account to and approves the correlation. The following settings are used for assigning approvers:

   Member List

   Assigns a reviewer based on attributes of the imported account. Imported endpoint accounts are stored as resources, so specify resource attribute mapping when you create this list.

   Default Assignee

   Specifies the default reviewer for all review actions that result from the correlation logic.

5. (Optional) Export correlation rules or synonyms to xml files. You can edit these files offline or upload them to create correlation rules for other endpoints.
   - To export correlation rules, click Export Rules to XML under Correlation Rules.
   - To export synonyms, click Export Synonyms under Manage Synonyms.

   Note: Saved correlation rules are only applied to new users and new accounts during the next import. To apply the rule to all accounts, start a full correlation.
6. Click Apply or Save.

   Account correlation rules are defined.

   Note: The accounts that are correlated are imported from endpoint connectors that are of merge type "As Accounts".

Correlate Account Options

CA GovernanceMinder executes account correlation logic automatically when it imports data, as follows:

- Users can have several accounts, but each account is mapped to a single user.
- When CA GovernanceMinder imports new accounts, it tries to match them to users.
- When CA GovernanceMinder imports new users, it tries to match them to unmapped accounts.

You can manually control account correlation with the following options in the Correlation tab of the Universe screen:

Un-Correlate All

Removes all links, except for CA IdentityMinder users, that map users to accounts and related resources in the Accounts configuration.

Start Full Correlation

Applies correlation logic to users and accounts in the universe. Existing mappings are preserved.

Advanced Comparator Options

The comparator specifies how user and account values are compared. In addition to standard string matching options, the following advanced options let a condition find near, inexact matches.

Note: These options can return false matches, especially when combined with synonyms.

Near Match Within One Character

Treats strings with a one-letter difference as a match. A letter can be changed, added, or missing from the string. For example, the following strings match the string Liza:

- Lisa (one changed letter)
- Liz (one missing letter)
- Eliza (one added letter)

Near Match Within Two Characters

Treats strings with up to two different letters as a match. Letters can be changed, added, or missing from the string. For example, the following strings match the string Lynne:

- Lynn, Wynne (single letter difference)
- Lynda (two changed letters)
- Lyann (one added letter, one missing letter)
- Luanne (one changed letter, one added letter)

Near Match Within Three Characters

Treats strings with up to three different letters as a match. Letters can be changed, added, or missing from the string. For example, the following strings match the string Margret:

- Margaret (single letter difference)
- Margarete (two-letter difference)
- Margarita, Maigrette (one changed letter, two added letters)
- Margarethe (three added letters)
- Margot (one added letter, two missing letters)
- Margery (three changed letters)

Implicit Accounts

When a universe does not have account configurations, or a user has no accounts on external endpoints, account information is not available. CA GovernanceMinder creates an implicit account to relate resources to users even when account information is not available from external endpoints.

The following system parameters control implicit accounts:

implicit.accounts.enabled

Specifies if CA GovernanceMinder creates implicit accounts for users.

Valid values; True, False

Default: False

Note: We recommend using account correlation instead of enabling this feature.

implicit.accounts.field.name

Specifies the field of user records that is used to name implicit accounts. Typically this is the loginID field.

implicit.accounts.field.name*universe_name*

Specifies the field of user records that is used to name implicit accounts in the specified universe. This value overrides the value of the implicit.accounts.field.name property for the specified universe.

Note: There is no period between name and *universe_name* in this field.

universe

Defines the universe that uses the field specified to name implicit accounts.

Implicit accounts have the following structure;

- The account name is taken from the field specified in the implicit.accounts.field.name property.
- The default mapped endpoint is taken from the Configuration resource application field specified for the universe.

Manage Accounts

When managing accounts in CA GovernanceMinder, you need the ability to do the following:

- View what user is correlated to what account
- Add correlations
- Clear correlations
- Change correlations

When an account comes from CA IdentityMinder or from a connector of merge type "As Users" or "As Users and As Accounts", the user of the account is read-only.

When an account comes from a connector of merge type "As Accounts", you can correlate the account to a user, clear the correlation, or correlate the account to a different user.

Follow these steps:

1. In the CA GovernanceMinder Portal, go to Administration, Accounts, Manage Accounts.
2. Select the universe with accounts you want to manage.
3. Review each account and its correlated users.

Export Data

CA GovernanceMinder export connectors export data to endpoint systems. For each import connector you define in CA GovernanceMinder, a matching export connector is automatically defined.

The Default Export connector appears when importing data from multiple endpoint systems. This option allows you to collect all the export data that is not exported through the Primary connector (CA IdentityMinder or CA IAM Connector Server) and pushes it to a custom executable file for export to a secondary endpoint.

To configure the Default Export connector, click the Not Exportable link under the Export Type column of the Connector (Export) screen. The following options are available:

- Custom Executable—allows you to write custom code that handles the remaining differences that are not exported
- Database Configuration—exports remaining differences to a database configuration
- Send Email—sends the remaining differences in two DIFF files (in client tool and XML formats) as attachments

Note: If you attempt to export a deleted user or resource from CA GovernanceMinder to CA IdentityMinder, CA GovernanceMinder removes all links from and to that user or resource. While the deletion action fails (it is not a supported action), CA GovernanceMinder still deletes all the links from and to the user or resource in CA IdentityMinder, as they are considered separate actions.

Run an Export with a Transformation

If you want to add to or modify your model before exporting the data, you can run a PDI transformation on the model prior to export. To manipulate the model, go to the Export connector screen under Export Flow Properties, and select a PDI transformation next to Set PDI Transformation on model.

Compare Configurations

A Role Engineer may examine the differences between two configurations to verify that the changes are correct before exporting.

The Compare Configurations option is a comparison that is made after discovery and audit processes are performed. The Master configuration from an endpoint is compared to the Model configuration, which is created while applying discovery and audit processes. In the final stage of the process, the Model configuration is exported to the endpoint, and the Master configuration is updated.

The Role Engineer has the option to display or not display the output, which is a Differences Report (DIFF file) or Updates Log.

Note: The Updates Log file and Differences Reports file, named DiffLog.txt and Diffreport.txt, can be opened at any time in a text editor for consultation or editing purposes.

Follow these steps:

1. In the Client Tools, click File, Compare Configurations.

   The Compare Configurations dialog appears.

2. Specify pathnames to input and output files.
3. Specify which differences to include in output files.
4. Specify report options as follows:

   View Report File

   Select this option to display a user-friendly report (Differences Report).

   View Updates Log

   Select this option to display the Updates Log.

5. Click Compare.

View the Status of an Import or Export Connector Job

To view the status of an import or export connector job, go to Administration, Workflows. This screen displays the status of the workflow process and whether it is still in progress or complete.

Chapter 4: Business Workflows

This section contains the following topics:

Business Workflow Overview

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 GovernanceMinder. Implementing these procedures in CA GovernanceMinder 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

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 GovernanceMinder 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 67).

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 68) 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 GovernanceMinder 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 GovernanceMinder.
   - 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.

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 68) during a certification. This option is only available for certification workflows.

Define and Send Escalation Emails

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

To define and send escalation emails

1. In the CA GovernanceMinder 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.

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.

Customize a Display Name

Property settings and fields establish which table columns can be linked to the Details (entity browser) popup dialog. The Details popup dialog enables you to view additional object details.

Determine these settings in the following locations:

- Universe

  The following occur at this location:

  - Effects table links displayed in the Entity Browser and the Actions List
  - Configured through the Portal Administration, Universes, Edit Universe

    The following fields enable you to set the data column linked to the Details popup dialog:

    - Configuration Users Display Name Field
    - Configuration Roles Display Name Field
    - Configuration Resources Display Name Field

- Certifications

  The following occur at this location:

  - Effects table links displayed in the certification screens only
  - Configured through the Portal Administration, Settings, Property Settings

    The following property settings enable you to set the data column linked to the Details popup dialog:

    - businessflows.inbox.display.field.USER
    - businessflows.inbox.display.field.ROLE
    - businessflows.inbox.display.field.RESOURCE

Default Workflow Action Options

You can control the tools that are available to business users when they handle items in their certification queue, or manage business workflows in their My Requests queue. The following system properties enable optional controls in these screens.

Note: These properties also affect the Workflow Administration screens used by administrators.

The following system property controls group handling of items in the certification screens:

businessflows.reviewers.default.allowSelectAll

Determines whether reviewers can handle all items in a table as a group. When this Boolean property is true, tables display check boxes in the Approve, Reject, and Reassign column headers. Reviewers select these check boxes to apply a decision to all the links in the table. This property also determines the default behavior for certifications: when this property is true, the Enable managers to select an entire column option in the Reviewers screen of the certification template wizard is selected by default.

The following system properties let users handle groups of items in the certification screens:

businessflows.inbox.approveRejectAll.enabled

Determines whether reviewers can approve or reject groups of items in the certification screens. When this Boolean property is true, the certification screen displays Assign and Reject columns. Users can approve or reject groups of items listed in the screen. They can also select check boxes in the Approve and Reject column headers to apply a decision to the entire contents of a table.

businessflows.inbox.reassignAll.enabled

Determines whether reviewers can reassign groups of actions in the certification screens. When this Boolean property is true, the certification screen displays the Reassign column. Users can reassign groups of actions listed in the screen. They can also select check boxes in the Reassign column headers to reassign the entire contents of a table.

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 GovernanceMinder 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 69).

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.

Chapter 5: Security and Permissions

This section contains the following topics:

Enabling Security

You can configure software security to behave in one of the following ways:

Default Permit

Under this condition, everything is permitted. This method enables greater functionality, and it can be adequate for the initial phases of setting up and testing the system.

Default Deny

Under this condition, everything that is not explicitly permitted is forbidden. While this method can improve security, it negatively affects functionality.

By default, CA GovernanceMinder Portal security is disabled. When a user logs in using a recognized user name, the Portal does not verify the user permissions and there are no limits on what the user can view and do.

Note: Configure external authentication before you verify built in accounts credentials.

You configure the type of security that is used in the Portal by setting a security parameter in the eurekify.properties file.

The security parameter resembles the following parameter example:

```
sage.security.disable=true
```

When you set this property to false, the product switches to the Default Deny security method. Only functionality that is explicitly permitted is visible and enabled for the user.

Encryption

When you send user login and password data, we recommend that you encrypt this data. The following is an encryption security parameter:

```
sage.security.disable.ssl.ADAuthentication=true
```

When you set this parameter to true, Secure Sockets Layer (SSL) authentication is disabled.

When you set the parameter to false and SSL encryption is enabled.

You supply the keystore file in the following security parameter:

```
sage.security.eurekify.keyStore.file=
```

The keystore file is a database that stores the private and public keys necessary for SSL encryption and decoding.

Administrator Password Encryption

The following administration accounts are created by default when you install the CA GovernanceMinder server:

- EAdmin—a default account with administrator privileges in the Portal.
- EBatch—a default account that is used to run batch processing jobs.

To secure these accounts, change their default passwords and encrypt the new password. Perform this procedure after you implement the desired encryption algorithms on the portal. For example, if your operating environment requires FIPS-compliant encryption, enable FIPS encryption algorithms before you encrypt these passwords.

Repeat this procedure when you change the active encryption algorithm of the CA GovernanceMinder server.

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

Follow these steps:

1. Click Administration, Settings, Properties Settings from the Portal.

   The Properties screen appears.

2. Enter the search term **password** in the Filter Properties Keys Containing field and click Apply Filter.

   A filtered list of properties appears.

3. Locate the following values in the list:

   sage.admin password

   Defines the password of the EAdmin user account.

   sage.batch.password

   Defines the password of the EBatch user account.

4. Modify and encrypt these passwords:

   a. Click Edit in the list to edit a property.

      The Edit Property window appears.

   b. Enter a new password in the Property Value field.

   c. In the Type drop-down list, select the Database Property option.

   d. Select the Encrypt Property check box, and click Save.

      The new password value is encrypted and saved to the database. Hash marks appear in the Property Value column of the Properties screen.

5. Repeat this procedure for both system properties.

   Administrator passwords are encrypted.

How To Enable FIPS 140-2 Encryption

Federal Information Processing Standards (FIPS) 140-2 is a US federal standard that dictates the security requirements for cryptographic modules that are utilized within a security system protecting sensitive information in computer systems.

The product makes limited use of encryption, primarily to protect passwords and other information that is used to access other applications, databases, or operating environments.

To enable FIPS 140-2 compliant encryption in CA GovernanceMinder, do the following:

- Implement Transport Layer Security (TLS/SSL) protection at the application server level.
- Provide an acceptable level of key (passphrase) security.

- Download and install Java security components.
- Configure the product to use FIPS-certified encryption algorithms. CA uses the RSA Crypto-J library for FIPS-compliant encryption.

Important! If FIPS-compliant encryption is adopted *after* the product begins to function, inconsistencies can result. Previously encrypted data can be rendered inaccessible, and passwords must be redefined. Select algorithms and a key storage method, and implement FIPS-compliant encryption immediately after installation, *before* you begin to work with the product.

Key Storage for FIPS-Compliant Encrpytion

A common issue in FIPS compliance is protection of the private key that is used for encryption. Software secured modules cannot protect the private key from someone who has root access to the system.

CA GovernanceMinder can support hardware-based key storage. However, implementation details differ for each hardware solution and cannot be described here.

The product supports the following software-based methods of key handling. Some provide adequate security for enterprise environments.

- **Embedded key**—by default the product uses an internal embedded key. The key is retrieved by calling the following Java class:

  com.eurekify.security.SimplePassPhraseGetter

  Use of this Java class ensures that the key is not stored in clear text. This method is not FIPS-compliant.

- **Key in File**—use this method when you require a customizable password. The password is stored in a text file named **password.txt** which is placed under the following directory:

  gm_install\Server\eurekify-jboss\conf

  Note: *gm_install* is the CA GovernanceMinder installation directory.

  The following Java class is used to retrieve the passphrase:

  com.eurekify.security.FilePassPhraseGetter

  The customer is responsible to secure the text file. This method is not FIPS-compliant.

- **Custom Passphrase Provider**—to support other solutions for key storage, you can implement a customized Java class. Your Java class must implement the following interface:

```
package com.eurekify.security;
public interface PassPhraseGetter {
/**
 * @return the passphrase used for the symmetric encryption
 */
public String getPassPhrase();
}
```

You specify one of the previous options by setting the **passphrase.getter.class** parameter when you configure FIPS encryption.

Password Tool

This FIPS-compliant password tool generates an encryption key from the command line. This functionality enables you to copy the generated FIPS key to an external file and use it for encryption.

The Password Tool is a ZIP file located in the following product package:

CA-RCM-12.6.01-CSM-Password-Tools.zip.

Follow these steps:

1. Edit the pwdtools.bat/pwdtools.sh file for a valid Java path.
   a. Locate and open the pwdtools.bat/pwdtools.sh file in an editor, and locate the following text:

      ```
      IF EXIST "%JAVA_HOME%" goto java_home_exists
      ```

   b. Replace the following with a valid Java path:

      ```
      %JAVA_HOME%
      ```

   c. Save and close the file.
2. Set the JAVA_HOME variable
3. Locate the following ZIP file in the CA GovernanceMinder package:

   ```
   CA-RCM-12.6.01-CSM-Password-Tools.zip.
   ```

4. In the Portal, navigate to Administration, Settings, Common Property Settings and add the following property:

   `fips.file.location=`*`fips_file_location`*

   Note: *fips_file_location* is the location of the external file generated by the CSM Password Tool using double backslashes (\\) in the path. For example:

   `c:\\sub_folder1\\sub_folder2\\Fipskey.dat.`

   If this property is not set, the product generates the FIPS key by default.

To use your external file for FIPS encryption with the product, go to the Portal and navigate to Administration, Settings, Comon Property Settings and add the following property:

fips.file.location=*fips_file_location*

where *fips_file_location* is the location of the external file generated by the Password Tool using double backslashes (\\) in the path, for example c:*sub_folder1**sub_folder2*\\Fipskey.dat. If this property is not set, the product generates the FIPS key by default.

Password Tool Syntax

This command has the following syntax:

```
pwdtools -[FIPSKEY|JSAFE|FIPS] -p [plain text] -k [key file location]
```

JSAFE

Encrypt a plain text value using non-FIPS algorithm.

Example:

```
pwdtools -JSAFE -p mypassword
```

FIPSKEY

Create a FIPS key file.

Example:

```
pwdtools -FIPSKEY -k C:\keypath\FIPSkey.dat
```

Where *keypath* is the full path to the location where you want the FIPS key to be stored.

The password tool creates the FIPS key in the location specified.

Note: Be sure to secure the key by setting the directory access permissions for specific group or user types.

FIPS

Encrypt a plain text value using a FIPS key file. This uses the existing FIPS key file.

Example:

```
pwdtools -FIPS -p firewall -k C:\keypath\FIPSkey.dat
```

Where *keypath* is the full path to the FIPS key directory.

Install Java Components for FIPS on JBoss/Windows Servers

Download and install Java Cryptography Extension (JCE) to support FIPS encryption algorithms.

Note: When you implement the CA GovernanceMinder server using the IBM WebSphere application server on AIX, install a different package.

When you implement the CA GovernanceMinder server on a JBoss cluster, install JCE on each server in the cluster. You can install JCE on the initial server image before you create the cluster, or can repeat this procedure on each server of an existing cluster.

Follow these steps:

1. Browse to the following directory on the CA GovernanceMinder server:

   Java_home/lib/security

   Note: *Java_home* is the local home directory of the Java version the CA GovernanceMinder server uses.

2. Back up or rename the following files in this directory:
   - local_policy.jar
   - US_export_policy.jar
3. Browse to the Oracle Software Downloads site.
4. Download the Java(TM) Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files v6 package to the CA GovernanceMinder server.

   This package is provided in a file named **jce_policy-6.zip**.
5. Unzip the file.

   A new directory named **\jce** is created. Files are extracted to this directory.

6. Browse to this **\jce** directory, and copy the following files:
   - local_policy.jar
   - US_export_policy.jar
7. Paste these files in the following directory:

   Java_home/lib/security
8. In a clustered installation, repeat this procedure on each server in the cluster.

   Java components for FIPS on JBoss/Windows servers are installed.

Configure FIPS Encryption

Out-of-the-box, CA GovernanceMinder does not use FIPS-compliant encryption. You can enable FIPS-compliant algorithms and key handling to implement FIPS encryption.

Important! You need administrator level rights in the Portal to perform this procedure.

Follow these steps:

1. (JBoss 5.1) Explode ear and war files (see page 81).
2. In the CA GovernanceMinder portal, go to Administration, Settings.

   The Settings menu appears.
3. Click Common Properties Settings, and modify these parameters:

   pbe.fips.enabled

   Specifies if CA GovernanceMinder uses FIPS-compliant encryption algorithms.
   - **True**—Use FIPS-compliant encryption.
   - **False**—Use non-compliant encryption.

   passphrase.getter.class

   Defines the Java class that is used to retrieve the encryption key.

   pbe.provider

   Defines the provider of the FIPS-compliant algorithms. To use the RSA JSafeJCE algorithms that CA provides, leave this property blank. If you specify another provider, copy that algorithm set to all computers running the CA GovernanceMinder server.

   Note: To save changes to a property, select Database Property from the Type drop-down list, and click Save.
4. Restart the CA GovernanceMinder server or server cluster.

JBoss 5.1 FIPS Configuration

As a known issue in JBoss 5.1, .ear and .war files must be in hierarchical form.

Follow these steps:

1. Stop the JBoss server and navigate to the JBoss 'deploy' folder.
2. In the JBoss 'deploy' folder, locate the tmsWPAdapter.ear and viewer.war files.
3. For the tmsWPAdapter.ear file in the JBoss 'deploy' folder:
    a. Create and name a folder tmsWPAdapter, and extract the contents of the tmsWPAdapter.ear file into it.
    b. Delete the original tmsWPAdapter.ear file.
    c. Rename the tmsWPAdapter folder as tmsWPAdapter.ear.

    The tmsWPAdapter.ear folder now contains the tmsWPAdapter.war file, and the APP-INF and META-INF folders.

    d. Under the tmsWPAdapter.ear folder, create and name a folder tmsWPAdapter, and extract the contents of tmsWPAdapter.war file into it.
    e. Delete the original tmsWPAdapter.war file.
    f. Rename the tmsWPAdapter folder as tmsWPAdapter. war.
4. For the viewer.war file in the JBoss 'deploy' folder:
    a. Create and name a folder viewer, and extract the contents of viewer.war file into it. Delete the original viewer.war file.
    b. Rename the viewer folder as viewer.war.
5. Delete the JBoss work, temp and data folders that are located next to the JBoss 'deploy' folder.
6. Start the JBoss server.

(JBoss) Adjusting Portal Session Timeout

The Portal session may cause performance and security issues in your deployment.

You can adjust the default timeout period to work around both issues. Edit the web.xml file to change the Portal session timeout period from the default setting.

Follow these steps:

1. Locate and open the web.xml file located in the following directory:

   gm_home/Server/eurekify-jboss/server/eurekify/deployers/jbossweb.deployer/

2. Locate and change the session configuration section timeout variable:

```
<session-config>
     <session-timeout>30</session-timeout>
 </session-config>
```

   Note: The unit of time is minutes.

3. Save changes to the file and close.

Permissions

When security is enabled in CA GovernanceMinder, every action a user attempts is verified against their permissions.

To enable security in CA GovernanceMinder, edit the permissions configuration file (eurekify.cfg). Each role in this configuration file represents a set of permissions. Each resource in the configuration file is a rule or filter that defines the scope of access to Portal functions or data. To give permissions to a user, associate the appropriate resources with a role and be sure that the user is a member of that role.

No permission filters exist for Delegate or Escalate functionality.

Note: An approver can view the contents of an Approver ticket, even if an administrator did not give the approver the appropriate permissions. CA GovernanceMinder defines resources to handle this issue in the background. These permissions are limited to that specific certification requirement.

Resources in the Permissions Configuration

To manage permissions for CA GovernanceMinder, create resources in the permissions configuration file (eurekify.cfg) using the client tools. The following types of resources are predefined in CA GovernanceMinder:

- Link Type resources—determine which menu options are visible to each user in the Portal.
- Doc_Access Type resources—determine level of access to CA GovernanceMinder document files, such as configurations, audit cards, universes, and so on.
- Filter Type resources—determine access to specific CA GovernanceMinder entities.

Create Resources in the Permission Configuration

To manage permissions for CA GovernanceMinder, create resources in the permissions configuration file (eurekify.cfg).

To create resources in the permissions configuration file

1. Verify that the database server and the CA GovernanceMinder server are running.
2. In the client tools, click File, Review Database.

   The Database Wizard appears.
3. Select the Eurekify.cfg file, clear the Write Protected check box, and click Open.

   The Eurekify.cfg file appears. Each role in this configuration file represents a set of permissions. Each resource is a rule or filter that defines the scope of access to Portal functions or data.
4. Click the Resource Database icon or click View, Resource Database.

   The resource database associated with the configuration appears in a new window.
5. In the resource database window, right-click and select Add Resource.

   The Resource Details screen appears.
6. Fill in the fields appropriately, depending on the resource type you are adding (Link, Doc_Access, or Filter.)
7. Click OK.
8. Repeat Steps 6 through 8 for every resource you want to add.

9. Add the new resources to the configuration file, as follows:
    a. Select a new resource and drag it to the resource section of the Eurekify.cfg window.

       The cursor changes into an ADD icon.

    b. Release the cursor.

       The new resources are added to the configuration file.
10. Save changes to the Eurekify.cfg file.

Link Type Resources

Link resources determine which menu options are visible to each user.

The general syntax is as follows:

[*Menu_Name.sub_menu*]

Enter the resource syntax in the Res Name 1 field.

For example, [Self-Service.*] allows users linked to this resource permission to see and use all the available Self-Service menus.

Adding [EX] after the square brackets excludes a specific menu or menu item from the user's menu options.

For example, to exclude the Request New Role menu item, use the following syntax:

[SelfService.requestNewRole][EX]

Doc_Access Type Resources

Doc_Access resources determine access to CA GovernanceMinder document files, such as configurations, audit cards, universes, reports, and so on.

The general syntax is as follows:

[*document_type*][*access_level_type*]

Enter the resource syntax in the ResName 1 field.

For example, [AUDITCARD] allows users linked to this resource permission to access this type of file. Adding the modifier, such as [RW], sets the level of access to the document type specified.

The following access level types are available:

- CREATE [C]—allows a user to create (or copy) the document type specified. Can be used with MEMBERLIST and CAMPAIGN document types.

  Note: When adding a certification permission, ResName 2 must be the universe name, not the certification name.

- MANAGE [RW]—allows a user to manage the document type specified.
- VIEW [R]—allows a user to view the document type specified.

Note: CREATE [C] includes the VIEW and MANAGE permissions. MANAGE [RW] includes the VIEW permission.

The value entered in the ResName 2 field influences the level of permissions. An asterisk (*) indicates full permissions for all such files, or a specific entity, such as a configuration name, universe name, and so on, can be listed.

Filter Type Resources

Filter resources determine access to specific CA GovernanceMinder entities. Filters are based on the standard LDAP filter format.

When you add a Filter resource to CA GovernanceMinder, you can use the following filters:

- [Filter_User]
- [Filter_Role]
- [Filter_Resource]

Populate the following additional fields when using a Filter resource:

Res Name 1

Specifies the filter to use: Filter_User, Filter_Role, or Filter_Resource.

Res Name 2

Specifies the universe name.

Res Name 3

Specifies the filter name or number.

Description

Specifies a description of the filter.

Type

Defines the resource type: Filter.

Filter1

Defines the filter. For example, (>(type=role)(A(type=user)(sageUser=$$PersonID$$))).

Filter Format

Filters rely on the LDAP prefix filter format. The filter is constructed from an expression which, in turn, can be constructed from sub-expressions.

Parenthesis ("(",")") surround each filter expression and represents a set of CA GovernanceMinder entities.

The simplest form of a filter is a field-value pair consisting of a CA GovernanceMinder entity field name and a desired value with an equal sign between them. For example, "(Location=Cayman)" or "(PersonID=86.*)".

Another simple filter is (Name>Smith) which returns users whose Name field alphabetically follows Smith. Thus, a filter such as the following:

```
(&(UserName>C)(UserName<F))
```

returns users whose Name field falls between the letters C and F, including C and F.

You can also filter for entity matches. This filter starts with a tilde (~), and is an entity-value pair consisting of an CA GovernanceMinder entity type (user/role/resource) and a related entity name separated by an equal sign. For resources, three sets of parenthesis with the three pairs appear after the ~. For example:

```
(~(role=Cayman)) or (~(resname1=email)(resname2=outlook)(resname3=WinNT))
```

You can also filter to see all users that have a field value that equals the field value of the current user. A filter such as the following:

(Organization=$$Organization$$)

returns users whose Organization field value equals the field value of the current user.

Filters can also have logical operations applied to them. The available operators are AND, OR, and NOT. Operator symbols are as follows:

& - AND

| - OR

! – NOT

Operator symbols are prefixes and must be placed before the expression, for example:

```
"(&(Location=Cayman)(Organization=Finance))" - users in the Cayman Finance office

"(|(Country=US)(Country=UK))" – users in the US or the UK

"(!(Active=false))" – active users
```

Filters can be as complex as necessary, as long as they meet the previously listed rules. For example:

```
"(&(|(Country=US)(Country=UK))(&(!(Active=false))(Organization=Finance)))"
```

This filter returns all the active users that are from the US or the UK and in the Finance department.

Filter Extensions

These filter extensions are for use with certifications only. The following additional filters involve the RACI model:

A — approved entities

> — links to approved entities

For example:

- All roles whose approver is “AD1\Admin”

  ```
  (A(type=role)(sageUser=AD1\Admin))
  ```

- All roles linked to users whose manager is “AD1\Admin”

  ```
  (>(type=role)(A(type=user)(sageUser=AD1\Admin)))
  ```

Property: sage.security.filter.escapeRegex

sage.security.filter.escapeRegex

Defines whether regular expression characters in the filter are escaped.

When set to false, you can create a role filter such as 'rolename=Org.*' that enables you to view all roles that start with 'Org'. The asterisk (*) is read as a wildcard.

When set to true, you can create a role filter that includes a regular expression character in the role name. To filter for a role with a regular expression character, the character must be escaped in the permission configuration, for example, 'rolename=Org\.*'.

Default: False

Use Case: Member List Permissions by Universe

CA GovernanceMinder associates a member list with a specific universe. To add a permission that allows a user to create (or copy) new member lists for a specific universe named 'Demo', add the following doc_access resource in the permissions configuration file (eurekify.cfg):

[MEMBERLIST][C], Demo, *

A user without the CREATE permission does not see the Add Member List screen in the Portal. If you want the user to have modify permissions only, use the MANAGE [RW] permission.

Note the following:

- Member lists created before CA GovernanceMinder 12.5 SP5 are listed as unassociated with any universe. Any user with MANAGE or CREATE privileges in all universes (permission type MEMBERLIST with ResName 2 set to '*') can associate these member lists by editing the member list.
- Be sure to add the appropriate Link Type resource so the user can navigate to the Member List screens in the Portal.

Use Case: Certification Permissions by Universe

CA GovernanceMinder associates a certification with a specific universe. To create a permission that allows the creation of a certification on the universe named Demo, add the following Doc_Access resource in the permissions configuration (eurekify.cfg):

[CAMPAIGN] [C], Demo

Note: If you want to give permissions for many universes, but not all universes ('*' in ResName 2), create a permissions resource for each universe in the permissions configuration (eurekify.cfg).

A user without the CREATE permission cannot create a certification in the Portal. If you want the user to have modify permissions only, use the MANAGE [RW] permission.

Note the following:

- Be sure to add the appropriate Link Type resource so the user can navigate to the appropriate Certification screens in the Portal. For example, [Administration.NewCampaign]. The NewCampaign permission does not exist by default, but you can create it to enable access to this specific administration menu item in the Portal. Or, to enable all Administration menu items, you can use the permission [Administration.*].
- Be sure to add the appropriate configuration permission so the user can add a certification to the configuration. For example, [CONFIGURATION] [RW], *configuration_name.*
- Set the property sage.security.disable to false.

Use Case: Report Permissions by Universe

CA GovernanceMinder associates a report with a specific universe. To create a permission that enables the creation of a report on the universe that is named Demo, add the following Doc_Access resource in the permissions configuration (eurekify.cfg):

REPORT [Demo]

Access to all reports in the universe.

REPORT [Demo] [ReportName]

Access to a given report in the universe.

REPORT [*] [ReportName]

Access to all reports with the given name in any universe.

Note: To grant permissions for many universes, but not all universes ('*' in ResName 2), create a permissions resource for each universe in the permissions configuration (eurekify.cfg).

A user without the CREATE permission cannot create a report in the Portal. If you want the user to have modify permissions only, use the MANAGE [RW] permission.

Note the following:

- Be sure to add the appropriate Link Type resource so the user can navigate to the appropriate report screens in the Portal. For example, [Administration.NewCampaign]. The NewCampaign permission does not exist by default, but you can create it to enable access to this specific administration menu item in the Portal. Or, to enable all Administration menu items, you can use the permission [Administration.*].
- Be sure to add the appropriate configuration permission so the user can add a certification to the configuration. For example, [CONFIGURATION] [RW], *configuration_name.*
- Set the property sage.security.disable to false.

Assign a Resource to a Role

Assign resources to a role to give users of that role access to defined Portal permissions.

To assign resources to a role

1. In the Eurekify.cfg window in the client tools, select new resources and drag them to a role listed under the Role section of the window.

   The cursor changes into a LINK icon.

2. Release the cursor.

   The new resources are linked to the role specified in Step 1.

3. Right-click the role specified in Step 1 and select Show All Linked Entities.

   User and resource entities linked to the role are highlighted.

   Note: To add users to a role, select the user in the User section of the Eurekify.cfg window and drag it to a role listed under the Role section of the window.

4. Verify that the new resources are linked to the role specified in Step 1.
5. Save changes to the Eurekify.cfg file.

Assign a User to a Role

Assign users to a role to give users access to entitlements defined in the role.

Follow these steps:

1. In the Eurekify.cfg window in the client tools, select the user in the User section and drag it to a role listed under the Role section of the window.

   The cursor changes into a LINK icon.

2. Release the cursor.

   The new user is added to the role specified in Step 1.

3. Right-click the role specified in Step 1 and select Show All Linked Entities.

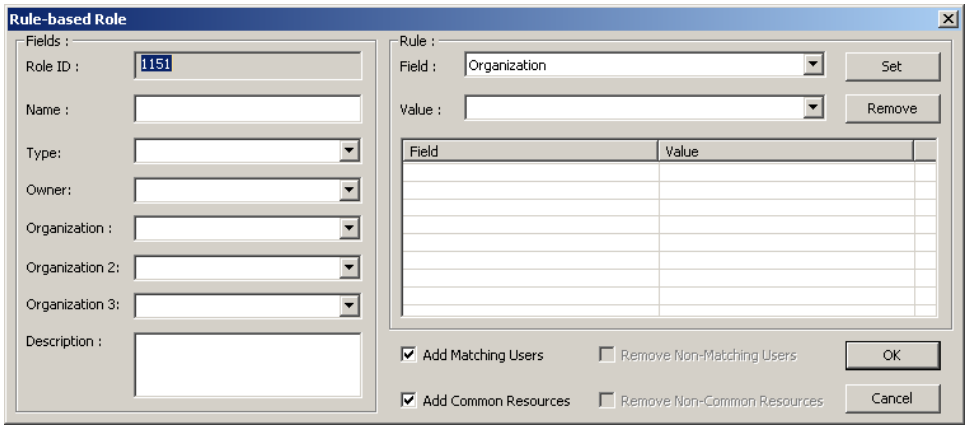
   User and resource entities linked to the role are highlighted.

4. Verify that the new user is linked to the role specified in Step 1.
5. Save changes to the Eurekify.cfg file.

Assign Users using Rule-based Roles

Rule-Based roles employ a set of organizational, functional, and hierarchical based characteristics to define a rule that is then used to assign users with matching characteristics to the role. Using a rule-based role, you can scan the entire configuration and identify all users that conform to the role in one single action. Rules-based roles are constructed and added to the configuration through the Rule-based Role window.

Rules are made up of a series of Field and Value pairs, selected and then set in the Rule group box in the right side of the Rule-based Role window.



Follow these steps:

1. Click Edit, New Rule-based Role.

   The Rule-based Role window appears. The Role ID appears and is incremented by a value of 1 from the ID given to the previously created role.

2. Enter a Name for the role in the Name text field.

3. Populate the remaining edit fields in the Fields group box in the left part of the window. The operation is identical to that described for creating a regular role.

4. In the Rule group box, select a field type from the Field drop-down.

5. Select a corresponding value from the Value drop-down.

6. Click Set.

   The Field and Value pair are placed in the Rule list.

7. Repeat steps 4-6 to add another Field/Value pair to the rule.

8. Select the Add Matching Users check box to populate the role with all users that match the rule. The check box is selected by default.

9. Select the Add Common Resources to populate the role with all resources that match the rule.

   The check box is selected by default.

10. Click OK to save the Rule-based role.

    The role is added to the configuration file and is listed at the bottom of the configuration file Role Panel.

Use Case: Filter to Provide Self-Service Access to a User

To allow a user to access all of their own entities for self-service functionality, add the following filter type resources to CA GovernanceMinder using the client tools.

1. Add a user filter by filling out the Resource Details screen as follows:
   - Res Name 1: [FILTER_USER]
   - Res Name 2: *
   - Description: Users can see themselves in universes that use the LoginID field.
   - Type: Filter
   - Filter1: (user.LoginID=$$PersonID$$)
2. Add a role filter by filling out the Resource Details screen as follows:
   - Res Name 1: [FILTER_ROLE]
   - Res Name 2: *
   - Description: Users can see their linked roles in universes that use the LoginID field.
   - Type: Filter
   - Filter1: (~(user.LoginID=$$PersonID$$))

     Note: The tilda operator (~) specifies linked entities.
3. Add a resource filter by filling out the Resource Details screen as follows:
   - Res Name 1: [FILTER_RES]
   - Res Name 2: *
   - Description: Users can see their linked resources in universes that use the LoginID field.

- Type: Filter
- Filter1: (~(user.LoginID=$$PersonID$$))

Note: To avoid truncating the filter string, expand the width of the Filter1 column in the Edit Resource pop-up screen before you enter the string.

4. Enter a value for the Filter ID (Res Name 3) field for each new resource filter according to the numerical sequence.
5. Associate the new resource filters with a role.
6. Save changes to the Eurekify.cfg file.

Important! If you mapped the login ID attribute to an attribute other than LoginID in the universe, change LoginID to the correct attribute in the filter. For example, if login IDs are stored in the GUUID attribute, change the filter as follows:

(user.GUUID=$$PersonID$$)

Chapter 6: Authentication Options

This section contains the following topics:

Enable Active Directory Authentication

Authentication is the act of establishing that a user has sufficient security privileges to access the CA GovernanceMinder Portal. When you enable Active Directory authentication, the system authenticates users logging in to the Portal using the Active Directory directory.

Follow these steps:

1. In the the Portal under Administration, Settings, System Properties:

   The Properties Settings window appears.

2. Set these properties as follows:

   sage.security.disable.ADAuthentication

   Set this value to False to enable Active Directory authorization.

   security.ldap.server

   The *host_name* OR *active_directory_IP* (example: HOSTNAME.org.com).

   sage.security.credentials.expiration.seconds

   Defines the lifetime of the credentials expiration, in seconds. Set this value to 60.

   sage.security.eurekify.keyStore.file

   Set this property when using SSL and adding the AD certificate to a JVM keystore file.

   sage.security.eurekify.keystore.password

   Set this property when using a JVM keystore file for SSL.

   Note: Use separate instructions if you want to use a personal keystore instead of the JVM keystore.

sage.security.disable.ssl.ADAUthentication

Set this value to True to enable Active Directory authentication.

sage.default.domain

The *Active_Directory_domain*.

Note the following:

- You must have a Login ID filed in the database with the domain name (example: *domain*\jsmith)
- When logging in, the user must provide the Login ID (example: *domain*\jsmith). If the Active Directory domain is set as the sage.default.domain property, then domain is not required when logging in, only the Login ID (jsmith).

(Optional) security.manager.dn

The *AD_bind_account* (example: administrator).

Note: The DN may be required only when using SSL authentication.

(Optional) security.manager.password

The *AD_bind_account_password.*

You have enables Active Directory authentication.

Configure Active Directory with SSL Using a Personal Keystore

You configure Active Directory with SSL using a personal keystore.

Follow these steps:

1. Install openSSL.
2. Run the following command:

   `openssl s_client -connect AD_server:636`

3. Copy the following output (inclusive) to a certificate TXT file:
   ----BEGIN CERTIFICATE----
   to
   ----END CERTIFICATE----
4. Verify the certificate by running the following command:

   `keytool -printcert -file cert.txt`

5. Locate the JBoss server.keystore file under the following directory:

   `eurekify-jboss/server/eurekify/conf`

6. Add the certificate to the keystore with the following command:

   ```
   "%JAVA_HOME%\bin\keytool" -import -file cert.txt -keystore
   server.keystore -storepass 123456
   ```

7. Set the following properties in the server:

   - sage.security.eurekify.keyStore.file
   - sage.security.eurekify.keyStore.password

     It is also possible to use JVM properties for the previous settings (in the eurekify.bat file):

   ```
   set JAVA_OPTS=%JAVA_OPTS%
   -Djavax.net.ssl.keyStorePassword=changeit
   set JAVA_OPTS=%JAVA_OPTS%
   -Djavax.net.ssl.trustStore="eurekify-jboss/server/eurekify/conf
   /keystore.txt"
   ```

   You have configured Active Directory with SSL using a personal keystore.

Enable LDAP Authentication

When you enable LDAP authentication, the system authenticates users logging in to the Portal using the LDAP directory.

Follow these steps:

1. In the Portal, click Administration, Settings, Properties Settings.

   The Properties Settings window appears.

2. Set the following property files as follows:

   sage.security.disable.ADAuthentication

   Set this value to False to enable Active Directory authorization.

   security.ldap.server

   The LDAP network server name.

   security.manager.dn

   The LDAP network administrator username.

   security.manager.password

   The LDAP administrator password in your network.

   security.authentication.ldap.server

   The LDAP server host name.

security.authentication.ldap.manager.dn

The LDAP administrator name.

security.authentication.ldap.manager.password

The LDAP administrator password.

security.authentication.ldap.rootContext

The name of the LDAP root context <?>

security.authentication.ldap.disable.ssl

Specifies if SSL is enabled for CA Directory.

security.authentication.ldap.lookupAttribute

Specifies the LDAP object attribute to match against <?>

security.authentication.ldap.disable

Set this value to False to disable LDAP authentication.

You have enabled LDAP authentication.

Enable CA IdentityMinder Authentication

When you enable CA IdentityMinder authentication, the system authenticates users logging in to the Portal using CA IdentityMinder. To enable CA IdentityMinder authentication, set the following properties through the Portal under Administration, Settings, System Properties:

Follow these steps:

1. Run an import from CA IdentityMinder, as the authenticated user must exist in CA GovernanceMinder.
2. Edit these eurekify.properties files as follows:
   - sage.security.disable.IMAuthentication=false
   - sage.security.IMAuthentication.universe=*universe_name* (the universe where you imported the users in Step 1)
   - sage.default.IMdomain=<blank>

     Note: This property must remain blank.
   - (Optional) If you are using CA IdentityMinder authentication *and* Active Directory authentication: sage.security.disable.ADAuthentication=false

3. Restart CA GovernanceMinder.
4. Verify authentication by logging in to the Portal with an imported user.

Note the following use cases around CA IdentityMinder authentication:

- If CA IdentityMinder and CA SiteMinder® authentication are both enabled, authentication is accomplished through CA SiteMinder®.
- If CA IdentityMinder and Active Directory authentication are both enabled, authentication is accomplished through CA IdentityMinder unless CA IdentityMinder fails, then authentication moves to Active Directory.

Single Sign-On (SSO) with CA SiteMinder®

You can use CA SiteMinder® to support the Single-Sign-On (SSO) function for CA GovernanceMinder Portal users.

Users log in to a CA SiteMinder® environment and are authenticated once. Users then have access to additional systems without being prompted to log in again at each site. CA SiteMinder® maintains user credentials and a list of active sessions.

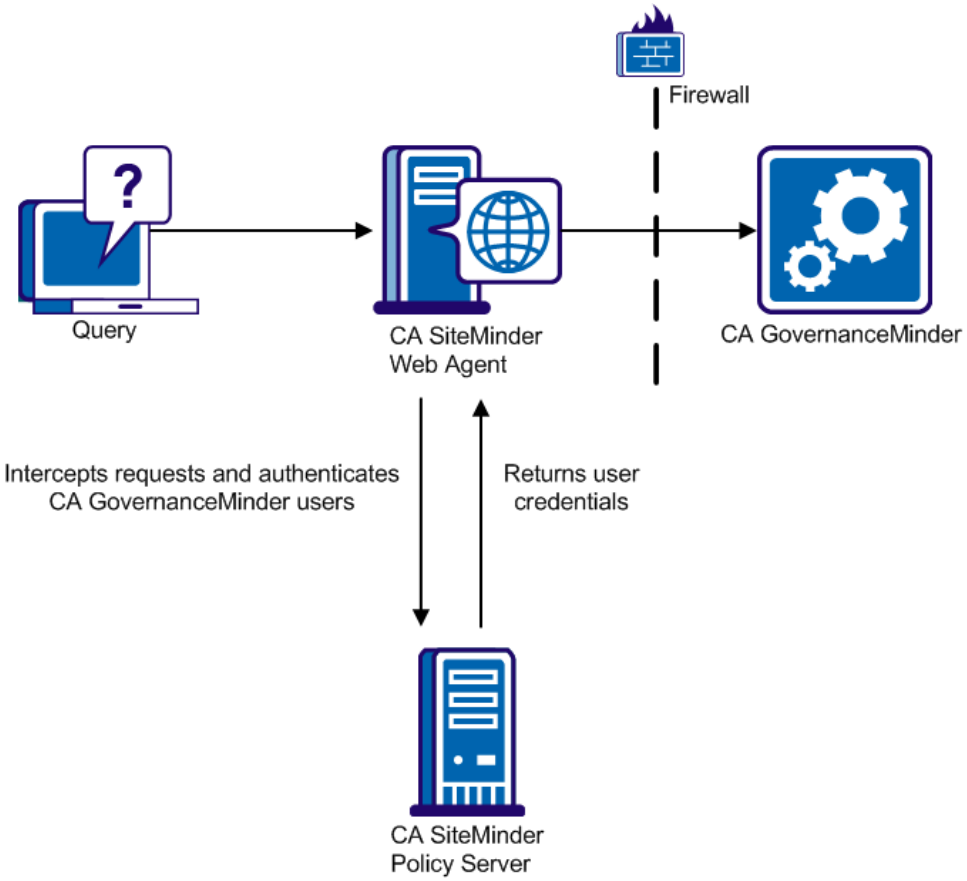
To implement SSO in the CA GovernanceMinder server environment, you must have the following CA SiteMinder® components:

- CA SiteMinder® Policy Server - This server authenticates CA GovernanceMinder users and returns information that identifies the user account in the CA GovernanceMinder Portal. Typically you implement SSO using an existing CA SiteMinder® Policy Server in the network environment.
- CA SiteMinder® Web Agent - This agent intercepts user requests that are sent to the CA GovernanceMinder Portal and authenticates CA GovernanceMinder Portal users. Install the Web Agent on an HTTP server or cluster that is compatible with CA SiteMinder® and sized to handle portal traffic. We recommend that you use the Apache HTTP server. You can use an existing CA SiteMinder® Web Agent, or you can install the agent on an HTTP server or a CA SiteMinder® compatible cluster.

When you implement SSO, a CA SiteMinder® Web Agent intercepts user requests submitted to the CA GovernanceMinder server, and queries the CA SiteMinder® Policy Server to authenticate the user. The Policy Server returns user credentials that enable the CA GovernanceMinder server to identify the user in the local portal users file.

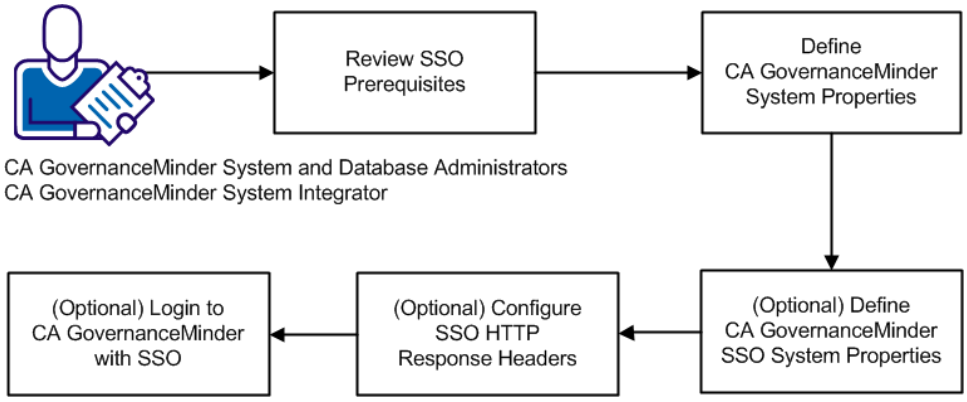
The CA GovernanceMinder and CA SiteMinder® servers are typically located behind enterprise firewalls, and the HTTP server with the CA SiteMinder® Web Agent is exposed to the public network.

The following diagram illustrates the CA SiteMinder® and SSO interaction:



Note: For more information about CA SiteMinder® implementation and configuration, see the *CA SiteMinder® Policy Server Configuration Guide*, the *CA SiteMinder® Web Agent Configuration Guide*, and other relevant portions of the CA SiteMinder® documentation.

The following diagram illustrates how to implement SSO with CA SiteMinder®:



Follow these steps to implement SSO with CA SiteMinder®:

1. Review SSO prerequisites.
2. Define CA GovernanceMinder system properties (see page 101).
3. (Optional) Define CA GovernanceMinder SSO system properties (see page 102).
4. (Optional) Configure SSO HTTP response headers (see page 103).
5. (Optional) Login to CA GovernanceMinder with SSO (see page 105).

Define CA GovernanceMinder System Properties

You define CA GovernanceMinder system properties to implement SSO, the web page where you direct users when they log out from the CA GovernanceMinder Portal, and to support CA SiteMinder® zones.

Follow these steps:

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

   The Property Settings window appears.

2. Define the following properties in CA GovernanceMinder:

   sage.security.SiteMinder.enabled

   This property specifies whether you implement SSO using CA SiteMinder®.

   Set to TRUE.

   logout.landingPageUrl

   This property sets the web page to where you direct users when they log out from the CA GovernanceMinder Portal.

   For an external CA GovernanceMinder Portal page, specify the full page URL. For an internal CA GovernanceMinder Portal page, specify only the page name, and omit the host, port, and portal pathname.

   Default value: loginForm

   sage.security.siteminder.cookie.*zone_name*

   This property specifies the session cookie name for each zone.

   Replace *zone_name* with the CA SiteMinder® zone name. Specify the cookie name as the value for the system property.

3. Save changes to CA GovernanceMinder system properties.

   You have defined CA GovernanceMinder system properties to implement SSO and support CA SiteMinder® zones. You have also defined the web page where you direct users to when they log out from the CA GovernanceMinder Portal.

   Next, you configure CA GovernanceMinder SSO system properties.

(Optional) Define CA GovernanceMinder SSO System Properties

You define CA GovernanceMinder system properties that control SSO operation to adjust system performance.

Follow these steps:

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

   The Property Settings window appears.

2. Define the following system properties that control SSO operation:

   sage.security.GUID.expiration.delta.seconds

   CA GovernanceMinder creates temporary proxy user IDs that support CA SiteMinder® user authentication. This property defines a cutoff time before the proxy ID expires, beyond which new requests are not sent using the ID.

   Default: 60 seconds.

   sage.security.GUID.expiration.minutes

   CA GovernanceMinder creates temporary proxy user IDs that support user CA SiteMinder® authentication. This property defines the lifetime of a proxy ID, in minutes.

   Default: 360 minutes (six hours).

3. Save changes to system properties.

   You have defined CA GovernanceMinder system properties that control SSO operation to adjust system performance.

   Next, you configure the SSO HTTP response header.

(Optional) SSO HTTP Response Headers

HTTP response headers are components of those HTTP message header fields that define the HTTP transaction operating parameters. The CA GovernanceMinder server maintains a configuration file (eurekify.cfg) that contains the CA GovernanceMinder Portal user accounts. You configure the CA SiteMinder® response policy to return the user information that corresponds to the UserID field in this configuration file as follows:

- The UserID field can contain the user name, for example:

  `Javier.Torres`

  In this example, the CA SiteMinder® response policy returns the user name as an HTTP header variable. You can use the standard, predefined **sm_user** CA SiteMinder® WebAgent-HTTP header variable attribute.

- The UserID field can contain the domain and username, for example:

  `GMusersDb\Javier.Torres`

  In this example, the CA SiteMinder® response policy returns both the domain and the username as HTTP header variables. Define a custom attribute, in one of the following ways:

  - Use the standard **sm_user** attribute for the username, and define a custom attribute for the domain.
  - Define a custom attribute that contains the entire domain\username value.

CA GovernanceMinder uses the following system properties to parse the returned HTTP header for returned attributes. These values must match the attribute labels that CA SiteMinder® inserts in the HTTP header:

sage.security.siteminder.username.attribute

Defines the attribute label in the returned HTTP header that contains the username or the value of the UserID field. The field defined in this property must be present in the HTTP header.

Default: sm_user

Note: This attribute is case-sensitive. Restart the system if you change the default setting.

sage.security.siteminder.domain.attribute

Defines the label of the attribute in the returned HTTP header that contains the user domain.

Default: rcm_domain.

Example: Domain and User Name in Separate Attributes

Consider the following UserID field in the CA GovernanceMinder user configuration file:

RCMusersDb\Javier.Torres

The returned HTTP header can specify this user using two attributes, with the following values:

```
sm_user="Javier.Torres" rcm_domain="RCMusersDb"
```

sm_user is a standard CA SiteMinder® attribute, but you define the *rcm_domain* attribute for the return policy.

To parse this header, both of the following CA GovernanceMinder system properties must be set to the default values:

- sage.security.CA SiteMinder®.username.attribute=sm_user
- sage.security.CA SiteMinder®.domain.attribute=rcm_domain

Example: Domain and Username in One Attribute

Consider the following UserID field in the CA GovernanceMinder user configuration file:

RCMusersDb\Javier.Torres

The returned HTTP header can specify this user using one attribute, with the following value:

```
rcm_userIDstring="RCMusersDb"
```

This attribute is not standard, and you define it for the return policy.

To parse this header, you only set the following CA GovernanceMinder system property:

- sage.security.CA SiteMinder®.username.attribute=rcm_userIDstring

Note: Not all environments include the domain name in the UserID field, but the username is always present. For this reason, CA GovernanceMinder always uses the **.username.** system property to parse the HTTP header, but the **.domain.** system property is optional.

(Optional) Login to CA GovernanceMinder with SSO

When you implement SSO, a CA SiteMinder® Web Agent intercepts and authenticates user requests for the default login page of the CA GovernanceMinder server. The following URL is the default login page of the CA GovernanceMinder server:

```
http://hostname:8080/eurekify/portal/login
```

Note: *hostname* is the IP address or the hostname of the CA GovernanceMinder server.

Authenticated users do not have to log in when they browse to this page.

In some cases, you want to log in locally on the CA GovernanceMinder server using a different user account. To log in directly to the CA GovernanceMinder Portal, browse to the following URL:

```
http://hostname:8080/eurekify/portal/loginForm
```

The CA GovernanceMinder server ignores CA SiteMinder® authentication for this page and requires a local login.

Note: CA SiteMinder® intercepts and authenticates requests for this page. Browse to this page with a user account that CA SiteMinder® recognizes.

How to Implement Single Sign-on (SSO) with CA SiteMinder®

When you implement SSO, a CA SiteMinder® Web Agent intercepts user requests submitted to the CA GovernanceMinder server, and queries a CA SiteMinder® Policy Server to authenticate the user. The Policy Server returns user credentials that let the CA GovernanceMinder server identify the user in its local file of portal users.

Note: For more information about CA SiteMinder® implementation and configuration steps, see the *CA SiteMinder Policy Server Configuration Guide*, the *CA SiteMinder Web Agent Configuration Guide*, and other relevant portions of CA SiteMinder® documentation.

To implement SSO for the CA GovernanceMinder Portal:

1. Configure an HTTP server or cluster to function in reverse proxy mode.

   Note: On an Apache HTTP server, configure the mod_proxy module. For more information, see the documentation for your HTTP server.

   The HTTP server/cluster passes user communication with the CA GovernanceMinder portal.

2. Configure firewalls, IP masks, and other security settings required in your network environment.

   The HTTP server/cluster communicates with the CA GovernanceMinder server and the CA SiteMinder® Policy Server.

3. Install and configure a CA SiteMinder® Web Agent on the HTTP server or cluster.

   The Web Agent intercepts end-user communication with the CA GovernanceMinder portal.

4. On the CA SiteMinder® Policy Server, define a domain, realm, and policy for the new Web Agent. Define a response that returns some user information as HTTP header variables.

   The values that CA SiteMinder® returns identify the user in the CA GovernanceMinder configuration file of portal users.

5. Enable SSO on the CA GovernanceMinder server by setting the following system property to True.

   sage.security.siteminder.enabled

   Specifies whether single sign-on using CA SiteMinder® is implemented.

   Valid values: True, False

6. Define the following system parameter:

   logout.landingPageUrl

   Defines the web page to which users are sent when they log out from the CA GovernanceMinder portal. For a page external to the CA GovernanceMinder portal, specify the full URL of the page. For a page in the CA GovernanceMinder portal, specify only the page name, and omit the host, port, and pathname of the portal.

   Default value: loginForm

7. (Optional) To tune the system performance, configure CA GovernanceMinder system properties that control SSO operation.

   Important! We recommend that you are familiar with these settings before you consider changing them.

   sage.security.GUID.expiration.delta.seconds

   CA GovernanceMinder creates temporary proxy user IDs to support user authentication by CA SiteMinder®. This property defines a cutoff time before the proxy ID expires, beyond which no new requests are sent using the ID.

   Default: 60 seconds.

   sage.security.GUID.expiration.minutes

   CA GovernanceMinder creates temporary proxy user IDs to support user authentication by CA SiteMinder®. This property defines the lifetime of a proxy ID, in minutes.

   Default: 360 minutes (6 hours).

Support SiteMinder Zones

To support CA SiteMinder® zones, configure the following system property to specify the session cookie name for each zone:

sage.security.siteminder.cookie.*zone_name*

Replace *zone_name* with the name of the SiteMinder zone. Specify the session cookie name as the value for the system property.

How to Configure the HTTP Response Header for Single Sign-on

A CA SiteMinder® Web Agent intercepts requests from users to the CA GovernanceMinder portal. CA SiteMinder® authenticates the user, and a CA SiteMinder® response policy returns an HTTP header that identifies the user account in CA GovernanceMinder.

The CA GovernanceMinder server maintains a configuration file of portal user accounts. Configure the CA SiteMinder® response policy to return the user information that corresponds to the UserID field in this configuration file:

- The UserID field can contain simply the user name, for example:

  `Javier.Torres`

  In this case the CA SiteMinder® response policy returns the user name as an HTTP header variable. You can use the standard, predefined **sm_user** CA SiteMinder® WebAgent-HTTP header variable attribute.

- The UserID field can contain the domain and username, for example:

  `RCMusersDb\Javier.Torres`

  In this case the CA SiteMinder® response policy returns both the domain and the username as HTTP header variables. Define a custom attribute, in one of the following ways:

  - Use the standard sm_user attribute for the username, and define a custom attribute for the domain.
  - Define a custom attribute that contains the entire domain\username value.

CA GovernanceMinder uses the following system properties to parse the returned HTTP header for returned attributes. These values must match the attribute labels that CA SiteMinder® inserts in the HTTP header.

sage.security.siteminder.username.attribute

Defines the label of the attribute in the returned HTTP header that contains the username or the value of the UserID field. The field defined in this property must be present in the HTTP header.

Default: sm_user

Note: This attribute is case-sensitive and requires a reboot of the system if you change the default.

sage.security.siteminder.domain.attribute

Defines the label of the attribute in the returned HTTP header that contains the user domain.

Default: rcm_domain.

Example: Domain and User Name in Separate Attributes

Consider the following UserID field in the CA GovernanceMinder user configuration file:

RCMusersDb\Javier.Torres

The returned HTTP header can specify this user using two attributes, with the following values:

```
sm_user="Javier.Torres" rcm_domain="RCMusersDb"
```

sm_user is a standard CA SiteMinder® attribute, but you define the *rcm_domain* attribute for the return policy.

To parse this header, both of the following CA GovernanceMinder system properties must have their default values:

- sage.security.CA SiteMinder®.username.attribute: sm_user
- sage.security.CA SiteMinder®.domain.attribute: rcm_domain

Example: Domain and Username in One Attribute

Consider the following UserID field in the CA GovernanceMinder user configuration file:

RCMusersDb\Javier.Torres

The returned HTTP header can specify this user using one attribute, with the following value:

```
rcm_userIDstring="RCMusersDb"
```

This attribute is not standard, and you define it for the return policy.

To parse this header, you only set the following CA GovernanceMinder system property:

- sage.security.CA SiteMinder®.username.attribute: rcm_userIDstring

Note: Not all environments include the domain name in the UserID field, but the username is always present. For this reason, CA GovernanceMinder always uses the **.username.** system property to parse the HTTP header, but the **.domain.** system property is optional.

Local Login with SSO

When you implement SSO, a CA SiteMinder® Web Agent intercepts and authenticates user requests for the default login page of the CA GovernanceMinder server. This page has the following URL:

`http://hostname:8080/eurekify/portal/login`

Note: *hostname* is the IP address or hostname of the CA GovernanceMinder server.

Authenticated users do not have to log in when they browse to this page.

In some cases, you want to log in locally on the CA GovernanceMinder server using a different user account. To log in directly to the CA GovernanceMinder portal, browse to the following URL:

`http://hostname:8080/eurekify/portal/loginForm`

The CA GovernanceMinder server ignores CA SiteMinder® authentication for this page and requires local login.

Note: CA SiteMinder® intercepts and authenticates requests for this page. Browse to this page with a user account recognized by CA SiteMinder®.

Enable Authentication to Workpoint Server

You can enable authentication to the Workpoint server.

Follow these steps:

1. See your Workpoint documentation and enable authentications on the Workpoint server side.
2. Define the Workpoint user and password in CA GovernanceMinder by setting the following properties:
   - workpoint.connection.username
   - workpoint.connection.password

Note: The "workpoint.connection.username" value can be a specific username such as "Workpoint", or a pattern such as "workpoint-user-%d". The pattern option is useful when you want each connection to the Workpoint server to use a specific username.

Chapter 7: Integrating CA GovernanceMinder with Other CA Products

This section contains the following topics:

CA IdentityMinder Integration

CA IdentityMinder is an identity lifecycle management product that enables you to manage user identities and govern what they can access based on their role.

CA GovernanceMinder is an identity lifecycle management product that enables you to develop, maintain, and analyze role models. The product also provides centralized identity compliance policy controls and automates processes that are associated with meeting compliance demands.

When you integrate CA IdentityMinder and the product, you can do the following actions:

- Validate that CA IdentityMinder user privileges are granted according to business compliance policies
- Get suggested roles and compliance checking when creating or modifying CA IdentityMinder users, roles, and accounts
- Understand what roles exist in your organization, establish a role model that fits your organization, and re-create the desired role model within CA IdentityMinder
- Analyze and maintain the role model as the business evolves

Note: For more information about integration between CA IdentityMinder and the product, see the *CA IdentityMinder Integration Guide*.

CA User Activity Reporting Integration

With CA User Activity Reporting integration, you can import CA User Activity Reporting usage data into CA GovernanceMinder. CA GovernanceMinder then displays this usage data during certifications. Applications in CA User Activity Reporting correspond to resources in CA GovernanceMinder. CA User Activity Reporting records user access to an application and CA GovernanceMinder then retrieves this usage data to display during a certification.

For example, before you certify user access to a resource (application), you can review the usage data on how often the user actually accesses the resource.

You enable CA GovernanceMinder integration with CA User Activity Reporting per universe.

Perform the following process to enable CA User Activity Reporting integration:

1. Review the prerequisites for CA User Activity Reporting integration (see page 113).
2. Configure communication between CA GovernanceMinder and CA User Activity Reporting, as follows:
   a. Import CA GovernanceMinder queries into CA User Activity Reporting.
   b. Create a CA User Activity Reporting security certificate in the keystore of the CA GovernanceMinder server.
   c. Register CA GovernanceMinder on the CA User Activity Reporting server.
   d. Update CA GovernanceMinder properties.
3. Map data between CA GovernanceMinder and CA User Activity Reporting, as follows:
   a. Set the application attribute in the CA GovernanceMinder Universe.
   b. Map CA User Activity Reporting applications to applications in the CA GovernanceMinder universe.
   c. Update usage data from CA User Activity Reporting to CA GovernanceMinder.
4. To confirm feature setup, open a configuration of the universe in the entity browser, and verify that usage icons appear for users and resources.

Prerequisites for Integration with CA User Activity Reporting

Before configuring CA GovernanceMinder and CA User Activity Reporting to work together, be sure to do the following:

- Be sure that you have a working CA GovernanceMinder universe with imported CA GovernanceMinder entities. If you are using CA IdentityMinder in your environment, account information is automatically imported. If you are not using CA IdentityMinder, create an 'As Accounts' connector mapped to the endpoint that CA User Activity Reporting is monitoring, and use CA GovernanceMinder correlation rules (see page 54) to match the accounts to the user.

  Note: The application attribute should be set to ResName2 if you use the 'As Accounts' connector for account information.

- Install CA User Activity Reporting and create a user with permissions to view events.
- If necessary, create event sources (applications) in CA User Activity Reporting. Applications correspond to resources in CA GovernanceMinder. CA User Activity Reporting records user access to an application and CA GovernanceMinder then retrieves this usage data to display during a certification.

  Note: For more information about creating CA User Activity Reporting event sources, see the *CA User Activity Reporting* documentation.

Import CSV Data into an Account Configuration

If you have a legacy connector or only an 'As Users' connector in your universe, you can manually import account information from a CSV file into a special configuration that relates to the Model configuration of the universe.

Note: Because file-based import is a one-time process, only use a CSV file for initial import or occasional administrative updates to account information, and only when creating an 'As Accounts' connector is not preferred.

Follow these steps:

1. Prepare the data file.
2. Click Administration, Accounts, Import Accounts (Legacy) from the main menu of the Portal.

   The Import Accounts (Legacy) screen appears.
3. Specify the target universe and the CSV file to import, and click Import.

   The product copies new, unique records from the CSV file to the Account configurations. Existing information in the Account configurations is preserved.
4. (Optional) To verify imported account data, view the model configuration in the entity browser or open the account configurations in the Data Manager application

CSV File Structure

Each record of the CSV accounts data file must contain the following fields:

PersonID

Defines the user in the target universe who owns the imported account. This field has the same content and format as the PersonID field in the universe.

Endpoint

Defines the name of the endpoint that hosts the account. This field has the same content and format as the Configuration resource Application field specified for the universe.

Account

Defines the account name as it is exists on the endpoint.

The first line of the CSV file must be the following header:

```
personID,endpoint,account
```

Each line of the file must contain three values, separated by commas.

Example: CSV acounts data file

The following example shows a CSV file with four data records. The first two records map accounts to the same user, John Meade:

```
personID,endpoint,account
5467238,UNXMARKT,jmeade
5467238,NT-Security,john_meade
7635097,RACFTEST,marcus432
6523876,NT-Security,kim_bell
```

(Optional) Increase File Handles

In Unix, increase CA User Activity Reporting default number server file handles when integrating with the product. The default file handles limit the opening of too many files that can exhaust system resources. The CA User Activity Reporting server is only supported on Linux.

Follow these steps:

1. On the CA User Activity Reporting server, navigate to the following location:

   /etc/security/

2. Edit the limits.conf file. Look for the following caelmservice settings:
   - caelmservice soft nofile 4096
   - caelmservice hard nofile 4096
3. Change both caelmservice settings to 8192.

   You have increased file handles on the CA User Activity Reporting server.

Import CA GovernanceMinder Queries Into CA User Activity Reporting

To import CA User Activity Reporting usage data into CA GovernanceMinder, add the CA GovernanceMinder data queries to the CA User Activity Reporting query list.

Follow these steps:

1. Log in to CA User Activity Reporting as an administrator.
2. Navigate to Queries and Reports, Queries.
3. Under Query List, click Options, Import Query Definition.
4. Specify the RCM_Queries.xml file located in the following directory of the CA GovernanceMinder server:

   gm_install\Server\ELM

   Note: *gm_install* is the CA GovernanceMinder installation directory.

   CA User Activity Reporting imports the queries.

CA GovernanceMinder calls these queries to display CA User Activity Reporting query results when users click monitored resources.

Modifying SQL Queries for Certain Endpoint Types

An advanced integration option allows you to change the way CA GovernanceMinder counts endpoint usage data from CA User Activity Reporting. The default filter counts all kinds of login events, but you may decide that you only want to count certain login events. For example, if you have an SAP system and you only want to count events of a specific SAP transaction type.

Also, you may have some endpoints that provide a different type of event, for example, an endpoint with session creation events, and you want to count those events instead of login events.

In the previous use cases, you can change the default filter for your scenario, but it must comply with SQL WHERE clause syntax, using fields defined in the CA User Activity Reporting Common Event Grammar Guide.

For example:

```
(event_action = 'Login Attempt') AND (event_result = 'S')
```

Create a CA User Activity Reporting Security Certificate

To communicate with CA User Activity Reporting, create a CA User Activity Reporting security certificate and update the keystore with the new certificate.

Note: The following steps are specifically for Internet Explorer 8. If you use another browser, see that browser's documentation on creating a security certificate.

Follow these steps:

1. From the CA GovernanceMinder server, use Internet Explorer to log in to the CA User Activity Reporting API portal. Use the following URL to access the API portal:

   https://*calm_hostname:port*/spin/calmapi/calmapi.csp

   A security certificate error appears.

2. Click Continue to this website.

3. Click Certificate Error, View certificates.

   The Certificate dialog appears and displays information about the CA User Activity Reporting security certificate.

4. Click the Details tab and select Copy to File.

   The Certificate Export Wizard appears.

5. Export the certificate using the wizard, as follows:
   a. In the Export Format screen, select Base-64 encoded X.509 (.CER).
   b. Set the file name for the certificate to 'elm_cer.cer'.
   c. Click Finish.

   The certificate is saved on the CA GovernanceMinder server.
6. Update the keystore with the certificate, as follows:
   a. Open a command prompt on the CA GovernanceMinder server.
   b. Navigate to the directory that contains the exported certificate.
   c. Enter the following command:

      "%JAVA_HOME%\bin\keytool.exe" -import -file "*pathname_cer*" -keystore "%JAVA_HOME%\jre\lib\security\cacerts" -trustcacerts

      where *pathname_cer* is the pathname of the exported certificate.

      You are prompted for a password.
   d. Enter the following password, or the default cacerts password for your system:

      'changeit'
   e. At the prompt, enter y and press Enter.

   The CA User Activity Reporting certificate is installed in the keystore.
7. Verify that the new certificate appears, as follows:
   a. Enter the following command:

      "%JAVA_HOME%\bin\keytool.exe" -list –keystore "%JAVA_HOME%\jre\lib\security\cacerts"
   b. Enter the cacerts password.

      A list of certificates appears.
   c. Verify that the new certificate appears in the list.
8. Restart the application server hosting CA GovernanceMinder.

Register CA GovernanceMinder on the CA User Activity Reporting Server

To enableCA User Activity Reporting to recognize the CA GovernanceMinder server, register the product with the CA User Activity Reporting server.

Follow these steps:

1. Log in to the CA User Activity Reporting server as the *EiamAdmin* administrator, using the following URL address:

   https://*ELM_host*:5250/spin/calmapi/products.csp

   where *ELM_host* is the hostname of the CA User Activity Reporting server.

2. Under Registered Products, click Register.

   The New Product Registration window appears.

3. Enter the name and password you specified for the CA User Activity Reporting security certificate and click Register.

   The CA User Activity Reporting server recognizes the certificate and enables connection to the product.

Update CA GovernanceMinder Properties

For the CA GovernanceMinder server to communicate with CA User Activity Reporting, update the product system properties.

Follow these steps:

1. In the Portal, go to Administration, Settings, Property Settings.
2. Set the Property Keys filter for keys containing 'logmanager'.
3. Click Apply Filter.
4. Edit the following CA GovernanceMinder system properties:

   usage.import.logmanager.odbc.host

   Defines the hostname of the target CA User Activity Reporting server.

   usage.import.logmanager.odbc.port

   Defines the default CA User Activity Reporting database port.

   Default: 17002

   Note: To verify the database port CA User Activity Reporting is listening on, open Administrative Tools in Windows, and select Services, ODBC Server. Click the CA User Activity Reporting server and select the Server Listening Port field.

usage.import.logmanager.odbc.user

Defines the username of the CA User Activity Reporting account that CA GovernanceMinder uses to log in to CA User Activity Reporting. Must be an administrator account in CA User Activity Reporting or an account that has read access to everything.

usage.import.logmanager.odbc.password

Defines the password of the CA User Activity Reporting account that CA GovernanceMinder uses to log in to CA User Activity Reporting.

usage.online.logmanager.https.host

Defines the hostname of the target CA User Activity Reporting server.

usage.online.logmanager.https.port

Defines the listening port on the target CA User Activity Reporting server portal.

Default: 5250

usage.online.logmanager.https.certificate

Specifies the CA User Activity Reporting security certificate name that is provided when registering CA GovernanceMinder on the CA User Activity Reporting server.

5. Return to the Property Settings screen and set the Property Keys filter for keys containing 'accounts'.
6. Click Apply Filter.
7. Review the following CA GovernanceMinder properties. Usually these properties are left to their defaults, but they are useful to know about:

implicit.accounts.field.name

Defines the product attribute that is used to match against CA User Activity Reporting account IDs. If you want to match against another CA GovernanceMinder attribute, such as PMFkey or UUID, specify that attribute in this property.

implicit.accounts.enabled

Specifies if the automatic implicit matching of accounts occurs between the product and CA User Activity Reporting.

Default: True

Set the Application Attribute in the Universe

To map applications between CA GovernanceMinder and CA User Activity Reporting, first specify which ResName attribute within the CA GovernanceMinder Universe is associated with an application. **ResName2** is often the correct attribute, but this attribute depends on how data was imported into CA GovernanceMinder.

To define this attribute in the universe, go to Administration, Universes, and edit the universe. Under General, Configuration Resource Application field, select the attribute that defines the application.

Map CA User Activity Reporting Endpoints

You must map CA User Activity Reporting applications to CA GovernanceMinder resources. An event source or application in CA User Activity Reporting can correspond to an individual resource in CA GovernanceMinder.

Map applications in CA User Activity Reporting to each resource in the target CA GovernanceMinder universe. CA User Activity Reporting usage data is then correctly associated with CA GovernanceMinder resources.

Follow these steps:

1. In the CA GovernanceMinder Portal, go to Administration, Universes.

   The Universe screen appears.

2. Select the target universe.

   The Edit universe screen appears.

3. Under the Actual Usage tab, Settings, select Import and show usage data for this universe.

4. Click Refresh Usage Data.

   Note: You must first import data from CA User Activity Reporting to get a list of all applications before mapping the applications to CA GovernanceMinder resources.

5. Click the Application Mapping tab.

6. Map CA User Activity Reporting applications to CA GovernanceMinder, as follows:

   a. The left pane contains a list of all the applications in the CA GovernanceMinder Universe. Select a CA GovernanceMinder application.

   b. The right pane contains a list of all the applications in CA User Activity Reporting. Select the CA User Activity Reporting application you want to map to the selected CA GovernanceMinder application.

c. Click Add.

   Mapped applications appear in the center pane.

d. Repeat these steps for all applications.

7. Click Finish to save settings.

   You have mapped CA User Activity Reporting applications to CA GovernanceMinder applications.

Update Usage Data

When you import CA User Activity Reporting usage data for a universe, the usage data appears in all certification screens for that universe. Usage data also appears when you view a configuration of the universe in the entity browser.

To update usage data

1. In the CA GovernanceMinder Portal, go to Administration, Settings, Universe Settings.

   The Universe Settings screen appears.

2. Select the target universe.

   The Edit universe screen appears.

3. Click the Actual Usage tab.

4. To update CA User Activity Reporting usage data, select Import and show usage data for this universe.

5. (Optional) Define usage thresholds that determine the icon displayed in certification and entity screens.

   Based on these thresholds, resources are flagged as Frequently Used or Rarely Used, and users are flagged as Frequent Users or Occasional Users.

6. (Optional) Edit the default time period settings. If you expand the Time Periods pane, you can edit the default settings for Short, Medium, and Long time periods. Editing these values changes the available values in the 'days' drop-down list of the Thresholds pane.

7. Click Save.

8. Click Refresh Usage Details.

Traffic Limits for Usage Data

CA GovernanceMinder polls a CA User Activity Reporting instance for resource usage data and presents that data when you review or certify access privileges. When a large number of resources are tracked, polling CA User Activity Reporting generates a high volume of usage data. Traffic on the CA User Activity Reporting server increases, and the time interval for synchronizing usage data is lengthened.

Note: High traffic also impacts the time it takes to display detailed usage information when users click a usage icon during the access certification process or in the entity browser. In this case, a separate window opens in CA RCM, but the usage data make take significant time to load.

If time periods are minimized, but timeouts persist, change the value of the following system property to suit the size of the CA GovernanceMinder data universe and your operating environment:

usage.import.logmanager.odbc.timeout.seconds

Defines the waiting period for data queries from CA GovernanceMinder to CA User Activity Reporting. Increase the value of this property to support a higher volume of queries. When the volume of traffic at the CA User Activity Reporting server is high, use values of an hour (3600 seconds) or more.

Enable CA User Activity Reporting Online Links

CA User Activity Reporting event viewer online links are disabled in CA GovernanceMinder by default. If you want to enable CA User Activity Reporting online links, consider the following before enabling the feature:

- The CA User Activity Reporting user must be allowed to view CA User Activity Reporting events at some level.
- All CA GovernanceMinder users use the same CA User Activity Reporting user for the online link.
- Although the online link is filtered by accounts and endpoint, once the CA User Activity Reporting popup appears, the CA GovernanceMinder user can alter the local event filtering, therefore, a CA GovernanceMinder user can view any event that the CA User Activity Reporting user is allowed to view.
- CA GovernanceMinder only shows login events, but there can be other events on the endpoint that appear in other log files, that are not retrieved from CA User Activity Reporting when you click the event viewer link.

You can change the default behavior and enable CA User Activity Reporting online links by setting the following system property to true:

usage.online.logmanager.eventviewer.enabled

Update Mapping of CA User Activity Reporting Applications

Over time, new applications are added to CA User Activity Reporting. Similarly, new resources are added to the CA GovernanceMinder configuration, which represent new external applications. Update the application mapping in the universe periodically so that usage information is imported for these new resources.

Use the standard procedure to map new CA User Activity Reporting applications (see page 120).

Chapter 8: Optimizing CA GovernanceMinder

This section contains the following topics:

Resize the Memory Cache

When working with large configurations, increase the size of the CA GovernanceMinder server memory cache. This section describes how to resize the server cache memory.

To resize the memory cache, do the following:

1. Resize the Java virtual machine (JVM) memory heap.
   - JBoss (see page 125)
   - WebSphere (see page 126)
2. Reset the cache limits. (see page 127)

(JBoss) Resize the Java Virtual Machine Memory Heap

To support large configurations, you can expand the Java virtual machine (JVM) memory cache for the CA GovernanceMinder server.

Follow these steps:

1. Navigate to the following folders on the CA GovernanceMinder server:

   jboss_install\bin

2. Open the **run.bat** file for editing, and locate the following line:

   ```
   set JAVA_OPTS=%JAVA_OPTS% -Xms728m -Xmx1536m -XX:MaxPermSize=256m
   ```

3. To define the JVM memory heap settings, change the following parameters:

   -Xms

   Defines the minimum size of heap memory. For example, -Xms1200m sets minimum heap memory to 1.2GB. This memory is assigned at server start.

   Note: When using a 64bit JDK, and the available memory is greater than 1400M, set the -Xms parameter to use all available memory.

   -Xmx

   Defines the maximum size of heap memory. For example, -Xmx20g sets maximum heap memory to 20GB. This memory is assigned as needed.

   We recommend, for a 64bit system, that you allocate approximately 3GB of cache memory (RAM) for every 1,000,000 elements allowed in cache memory (3 * maxElementsInMemory (see page 127)).

4. Repeat this procedure on each server in the cluster.
5. Save and close the **run.bat** file.

   The Java virtual machine memory heap has been resized.

(WebSphere) Resize the Java Virtual Machine Memory Heap

To support large configurations, you can expand the Java Virtual Machine (JVM) memory cache for the CA GovernanceMinder server.

Follow these steps:

1. In the WebSphere Administrative Console, click Servers, Application Servers, and select a server in the cluster.
2. Click Process Definitions, Java Virtual Machine.
3. To define JVM memory heap settings, change the following fields:

   Initial Heap

   Defines the memory reserved for CA GovernanceMinder upon startup, in megabytes.

   Maximum Heap

   Defines the maximum memory that CA GovernanceMinder can use, in megabytes.

   We recommend, for a 64bit system, that you allocate approximately 3GB of cache memory (RAM) for every 1,000,000 elements allowed in cache memory (3 * maxElementsInMemory (see page 127)).

4. Repeat this procedure for each server in the cluster.

Reset Cache Limits

To support large configurations, you can expand the cache memory limits.

Cache memory is defined by the number of elements (users, resources, roles, and so on) that can be held in the cache at once. When the cache is full, elements are swapped in and out of memory, which can affect performance. The default setting limits the memory cache to 500,000 elements.

This procedure describes how to reset cache settings for an existing CA GovernanceMinder implementation. In WebSphere implementations, you can modify these settings before implementation by editing the EAR file you use to install the CA GovernanceMinder server.

Follow these steps:

1. Edit the **ehcache-sageDal.xml** file on the CA GovernanceMinder server:
   - For JBoss, this file is found in the following location:

     jboss_install\server\all\farm\eurekfiy.war\WEB-INF\classes\
   - For WebSphere, this file is located in the eurekify.ear file found in the following location:

     /eurekify.war/WEB-INF/classes
2. In the **defaultCache** entry, change the following attribute:

   maxElementsInMemory

   Defines the maximum number of elements stored in cache memory.

   We recommend that you set this field using the following formula:
   `maxElementsInMemory = total number of entities * 3`

   For example, if you have one universe with 500,000 users and 500,000 roles, set maxElementsInMemory to 3,000,000 elements.

   If you have two universes, each with 500,000 users and 500,000 roles, set maxElementsInMemory to 6,000,000 elements.
3. Save changes to the file and close.

   You have reset cache settings.

Cache Manipulation

Using the server cache improves performance. To improve performance, upload the current Universe and configuration data to the cache. Accessing the server cache is much faster than accessing the hard drives, so users can receive information more quickly when using a cache.

Load Cache

Use this utility to load a specific configuration into the server memory cache.

Follow these steps:

1. In the Portal, go to Administration, Cache, Load Cache.

   The Load Cache screen opens.

2. Select a Configuration from the drop-down list and click OK.

   The information bar indicates that the selected configuration is loaded.

Clear Cache

Use this utility when you update configuration data in the client tools, such as permissions, and you want to be sure that anyone using the system uses the updated data.

Follow these steps:

1. In the Portal, go to Administration, Cache, Clear Cache.

   The Clear Cache screen opens.

2. Click Clear Caches to clear the server memory cache.

   The information bar indicates that the selected configuration is loaded.

(JBoss) Adjusting Portal Session Timeout

The Portal session may cause performance and security issues in your deployment.

You can adjust the default timeout period to work around both issues. Edit the web.xml file to change the Portal session timeout period from the default setting.

Follow these steps:

1. Locate and open the web.xml file located in the following directory:

   gm_home/Server/eurekify-jboss/server/eurekify/deployers/jbossweb.deployer/

2. Locate and change the session configuration section timeout variable:

```
<session-config>
     <session-timeout>30</session-timeout>
 </session-config>
```

   Note: The unit of time is minutes.

3. Save changes to the file and close.

SQL Database Settings

To achieve the best performance, tune the following database settings:

Autogrowth

Set the Autogrowth properties for the all databases, as follows:

- File Growth Percent: 50%
- Maximum File Size: Unrestricted File Growth

Note: For more information about setting the Autogrowth properties, see the documentation for the database that you are using.

Tune the autogrowth property on the following databases:

- WPDS (workflow)
- SDB (eurekify_sdb)
- TicketDB (eurekify_ticketdb)
- ReportDB and I2DB (gvm_datawarehouse)

Maximum threads

Set the maximum worker threads to 12 threads per CPU in the MAX_THREADS setting in the GeneralMonitor.properties file.

The GeneralMonitor.properties file is installed in the following location by default:

*gm_install**app_server*\Workpoint

Note: If you performed a new installation, you do not need to modify these settings.

(Optional) After a large data import or purge, you may experience performance degradation. To improve performance, run the dbutil with the '-in' flag on the SDB database. This rebuilds the indexes in the relevant database.

Oracle Database Settings

When using Oracle as the CA GovernanceMinder database, some tasks may take a long time to complete. To improve the performance when using Oracle, consider the following recommendations:

- Processes: 500
- Session: 500
- REDO.log file size: 2GB each (there are 3)

- Memory: 4GB
- Tablespace datafile, varies as follows:

  TEMP—large amounts of data needs large amounts of temp space. Consider settings as follows:

  - Filesize: 1G
  - Automatically extend datafile, Increment: 200MB
  - Maximum File Size, Value: 20GB

  UNDO:

  - Filesize: 1G
  - Automatically extend datafile, Increment: 200MB
  - Maximum File Size, Value: 20GB

  USERS:

  - Filesize: 1G
  - Automatically extend datafile, Increment: 500MB
  - Maximum File Size: Unlimited

(Optional) When large amounts of data are inserted into the database, run the following statistics commands:

```
execute dbms_stats.gather_schema_stats('${SCHEMA}', DBMS_STATS.AUTO_SAMPLE_SIZE);

alter system flush buffer_cache;

alter system flush shared_pool;
```

Note: Replace *SCHEMA* with the database schema name (username).

Chapter 9: Configuring Additional Options

This section contains the following topics:

Do Not Remember Username at Login

The CA GovernanceMinder login screen now remembers usernames by default. The following property controls this functionality:

security.login.cookies.enable

Default: True.

If you do not want the login screen to remember usernames, set the property to False.

Define an Email Server

During role review and certifications, email messages are sent to managers throughout the enterprise. These emails prompt them to review access rights of the people and resources they manage. Specify an email host in the network that handles these emails.

Follow these steps:

1. Log in to the CA GovernanceMinder Portal as an administrator.
2. Click Administration, Settings, Properties Settings.

   The Properties window appears.
3. Edit the following system properties:

   mail.server

   Defines the network address of the email host that processes CA GovernanceMinder emails.

   mail.serverPort

   Defines the port CA GovernanceMinder uses to communicate with the email host.

Change the Default Port

If the application server port you want to use is not the default port, modify all properties using a URL to point to the new port.

For a cluster, use only the properties in the Properties Settings, which are external ports.

The Common Properties Settings are mostly for internal communication. Modify these properties only if you close the listening socket to the default port.

Change the following properties as necessary.

- Under Properties Settings:
  - sage.sageBaseUrl
  - reports.baseUrl
  - portalExternalLink.ticketQueueUrl
  - portalExternalLink.certificationUrl
  - portalExternalLink.homeUrl
- Under Common Property Settings:
  - statisticalService.url
  - reportsService.url
  - campaignService.url
  - sageBrowsingService.url
  - buildingBlockService.url
  - buildingBlockService.password
  - buildingBlockService.username

You can access these settings by going to Administration, Settings in the CA GovernanceMinder portal.

Rebrand the Portal

You can customize the branding of the Portal by replacing CA-branded text labels and graphics.

Note: Upgrading CA GovernanceMinder overwrites any customized portal graphics and text strings.

The following graphic files apply CA branding to the CA GovernanceMinder Portal:

- CAT_logo_53_trans.png
- CAT_logo_44_trans2.png
- brandstrip.png
- favicon.ico, a CA-branded favicon that is used to identify the CA GovernanceMinder Portal browser window.

The following graphic file applies to CA GovernanceMinder certification emails:

- logo.png

The following additional graphic file is bundled with the BIRT reporting tool, and applies CA branding to reports:

- LogoCustomerNewSmall.bmp

In addition, the Portal header texts are stored in CA GovernanceMinder server properties.

Rebrand the Portal on Windows/JBoss and WebSphere

To implement branding changes on a CA GovernanceMinder server on Windows/JBoss or WebSphere, overwrite files in the installation directory, edit a properties file, and in the local viewer.ear archive that is used by the BIRT reporting utility.

Follow these steps:

1. Prepare updated versions of the graphics and favicon files.
2. **Websphere:** Browse to the eurekify.war archive you used to install the CA GovernanceMinder server. Using Winzip or another file compression tool, open the file for editing.
3. In the CA GovernanceMinder installation directory, overwrite branded graphics files with updated versions.
   - The login logo and header images for the portal are located in the following folder under the installation folder:

     gm_install\Program Files\CA\RCM\Server\eurekify-jboss\server\eurekify\deploy\eurekify.war\images
   - The favicon for the Portal is located under the following folder:

     gm_install\Program Files\CA\RCM\\Server\eurekify-jboss\server\eurekify\deploy\eurekify.war

4. Edit the EurekifyBaseWebApplication.properties file that is located under the following folder:

   gm_install\Program Files\CA\RCM\Server\eurekify-jboss\server\eurekify\deploy\eurekify.war\WEB-INF\classes\com\eurekify\web\application

5. Replace the text strings in the following parameters:
   - portal.header.title
   - portal.header.fullTitle
   - portal.title
6. Save and close the EurekifyBaseWebApplication.properties file.
7. Repeat Steps 3, 4 and 5 for the EurekifyBaseWebApplication_*locale* file, depending on the locale of your browser, for example, EurekifyBaseWebApplication_en for English.
8. Save and close the files, and using Winzip or another file compression tool, recompress the eurikify.war archive.
9. Browse to the viewer.ear file located under the following folder:

   gm_install\Program Files\CA\RCM\Server\eurekify-jboss\server\eurekify\deploy
10. Using Winzip or another file compression tool, open the file for editing.
11. Overwrite the old graphics files in the archive with the updated versions.

    Note: Do not change the directory paths that are assigned to each file.
12. Save and close the viewer.ear file, and using Winzip or another file compression tool, recompress the viewer.ear archive.
13. **WebSphere:** Redeploy the eurekify.war and viewer.ear files using the WebSphere Administration Console.

    You have overwritten files in the CA GovernanceMinder installation directory and in the local viewer.ear archive that is used by the BIRT reporting utility.

Use Image Files in Entity Records

You can associate an image file with each user, role, or resource entity in the CA GovernanceMinder database. This file is displayed in information and certification screens of the CA GovernanceMinder Portal. Each image file is matched to an entity based on the value of an attribute field.

Follow these steps:

1. Plan implementation of image directories. Consider the following points:
   - You can reference existing image directories, or can create new directories locally on the CA GovernanceMinder server. Image directories that reside on other hosts in your network environment must be accessible to the CA GovernanceMinder server.
   - To select the image that corresponds to a specific user, role, or resource, use one or more user, role, or resource attributes. You can use existing attributes, or can create attributes for image mapping.
2. (Optional) If you use a new user, role, or resource entity attributes for image mapping, define them in the CA GovernanceMinder Portal or CA GovernanceMinder Client Tools.
3. In the CA GovernanceMinder Portal, click **Administration**, **Settings**, **Properties Settings** and edit the following properties:

   user.image.url

   Defines a URL template that lets CA GovernanceMinder retrieve an image for a specific user record. Typically this template combines the pathname of the image directory with wildcards for user attributes. In the following example, the /users directory on the CA GovernanceMinder server stores user images, and the userID attribute identifies individual images.

   `http://gm_host:port/users/$(userID).jpg`

   Note: *gm_host* and *port* are the CA GovernanceMinder server network address and communications port, and $(userID) is a placeholder for the actual value of the userID attribute.

   When CA GovernanceMinder displays the user record with userID value of 2384, it retrieves the file 2384.jpg from the target pathname.

role.image.url

Defines a URL template that lets CA GovernanceMinder retrieve an image for a specific role. Typically this template combines the pathname of the image directory with wildcards for role attributes. In the following example, the /roles directory on the CA GovernanceMinder server stores role images, and the userID attribute identifies individual images.

`http://gm_host:port/users/$(Owner).jpg`

Note: *gm_host* and *port* are the network address and communications port of the CA GovernanceMinder server, and $(Owner) is a placeholder for the actual value of the Owner attribute.

When CA GovernanceMinder displays the role with Owner value of 2384, it retrieves the file 2384.jpg from the target pathname.

resource.image.url

Defines a URL template that lets CA GovernanceMinder retrieve an image for a specific resource record. Typically this template combines the pathname of the image directory with wildcards for resource attributes. In the following example, the /resources directory on the CA GovernanceMinder server stores resource images, and the ResName3 attribute identifies individual images.

`http://gm_host:port/users/$(ResName3).jpg`

Note: *gm_host* and *port* are the network address and communications port of the CA GovernanceMinder server, and $(ResName3) is a placeholder for the actual value of the ResName3 attribute.

When CA GovernanceMinder displays the resource record with ResName3 value of Unix_admins, it retrieves the file Unix_admins.jpg from the target pathname.

Note: If you store the image files on the same server as the CA GovernanceMinder server, place the files in the following location:

`RCM_ROOT\Server\eurekify-jboss\server\eurekify\deploy\eurekify.war\images\`

Example: File location

The following example shows you where to place an image file for the user.image.url property:

`http://gm_host:port/$(userID).jpg`

4. (Optional) Create image directories corresponding to the pathnames you specified in the system parameters. Copy and rename image files to populate the directories.

5. (Optional) Replace the default images that CA GovernanceMinder displays when a user, role, or resource entity does not have a unique image file.

   For a CA GovernanceMinder server on Windows/JBoss, replace the images that are located under the following directory:

   gm_install\Server\eurekify-jboss\server\eurekify\deploy\eurekify.war\img

   Note: *gm_install* is the CA GovernanceMinder installation directory.

   Name the new image files as follows. Overwrite or rename existing files.

   - Default user image: User_Silhouette.gif
   - Default role image: UserGroup_48.png
   - Default resource image: Resource_48.png

Install Translated Portal Online Help Files

Translated versions of the online help files for the Portal are available from the CA Support site.

Follow these steps:

1. Download the ZIP file containing the translated online help files for the appropriate language from the CA GovernanceMinder product page on the Support site.

   Note: The translated online help files are posted *after* the GA version of the software. Typically, translated files are available from the Support site 60 days after the GA date.

2. Extract the contents of the ZIP file to a system that you can access from the CA GovernanceMinder server.

3. Copy the Portal folder from the ZIP file to the following location:

   gm_install\Server\eurekify-*appserver*\server\eurekify\deploy\eurekify.war\help\en

   Be sure to install the online help files in the **en** folder. The URL for the Portal online help is static, so the files must be in the specified directory to display correctly.

Set CA GovernanceMinder Date Format

The CA GovernanceMinder date and time format is set in property keys. You can change these formats by editing format property settlings.

Follow these steps:

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

   The Properties window appears.
3. Edit the following system properties:

   format.date.display

   Defines the CA GovernanceMinder format for the day month, year, hour and minute.

   format.onlyDate.display

   Defines the CA GovernanceMinder format for the day, month, and year.