CA GovernanceMinder

Scenario Guide

12.6.02

CA Technologies Product References

This document references the following CA Technologies products:

- CA GovernanceMinder
- CA Identity Manager
- CA SiteMinder®
- CA User Activity Reporting Module
- CA SDM

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: Scenario Overview

A scenario is concise information presented in the context of how a specific customer role interacts with a product to achieve a specific goal.

Scenarios represent a user case business process. They clearly identify customer roles involved, and explain the expected product behavior.

This section contains the following topics:

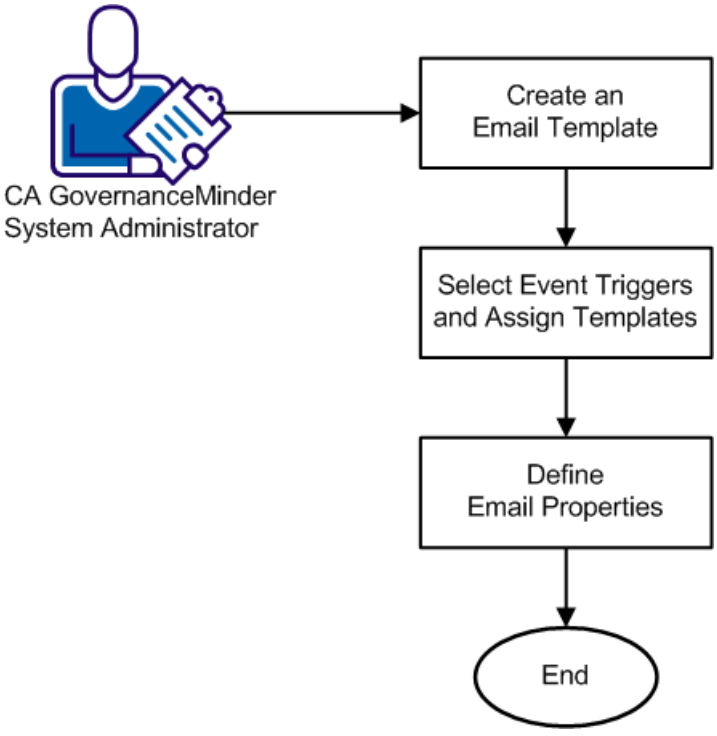
Chapter 2: How to Configure Email Notifications

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

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

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

The following diagram illustrates how to configure CA GovernanceMinder email notifications:



Follow these steps to configure CA GovernanceMinder certification email templates:

1. Create an email template (see page 10).
2. Select event triggers and assign templates (see page 11).
3. Define email properties (see page 12).

Create an Email Template

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

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

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

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

Follow these steps:

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

   The Email Templates screen appears.

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

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

     a. Click Load.

        The Load Template dialog appears.

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

        The template appears in an editing screen.

     c. Click Save As and rename the template.

   - Create a template:

     a. Click New.

        The New Template dialog appears.

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

c. Specify a template name in the Name field.

d. Click OK.

The Email Templates editing screen appears.

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

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

   You have created a custom email template.

Next, you specify certification events.

Select Event Triggers and Assign Templates

Specify certification events to generate CA GovernanceMinder certification emails.

Follow these steps:

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

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

   Note: This screen displays legacy events and templates from previous versions of CA GovernanceMinder. Legacy events are listed at the bottom of the table, and have separate Aggregation Templates. Do not activate these events.
2. Select the events that you want to trigger emails, and clear events that you do not want to trigger emails.

3. (Optional) Select an alternative template for the event in the Template drop-down list of the event.
4. Click Save to save settings.

   The selected events are enabled and templates assigned.

   Next, you define CA GovernanceMinder certification email properties.

Define Email Properties

Define CA GovernanceMinder email properties to customize email notifications.

Follow these steps:

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

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

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

   mail.Server

   Defines the SMTP server URL.

   Default: smtp.company.com

   mail.ServerPort

   Defines the communication port for the SMTP server.

   Default: 25

   mail.user

   Defines the CA GovernanceMinder user account on the SMTP server.

   Default: DemoV4@Eurekify.com

   mail.password

   Defines theCA GovernanceMinder account password on the SMTP server.

   Default: abc1234

   mail.from

   Defines the CA GovernanceMinder server originating email address.

   Default: RCM@ca.com

mail.useSSL

Specifies whether SMTP server communication uses SSL encryption.

Default: False

(Optional) mail.max.attempts

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

Default: 3

(Optional) mail.sending.interval

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

Default: 900 seconds

(Optional) mail.smtp.timeout

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

Default: 60 seconds

portalExternalLink.certificationUrl

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

portalExternalLink.homeUrl

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

3. Click Save.

You have defined the email properties.

Chapter 3: How to Define a 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).

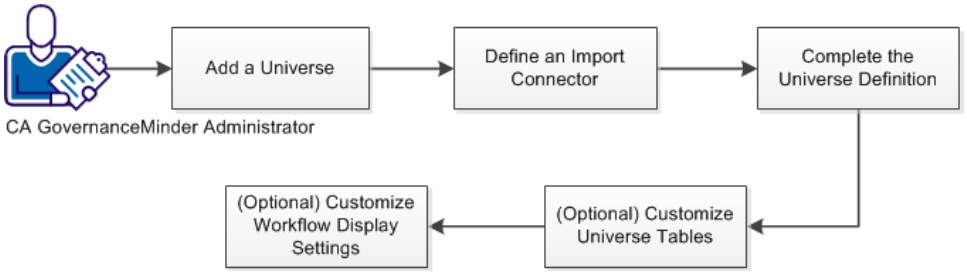
A CA GovernanceMinder universe stores imported endpoint data from such sources as CA Identity Manager, [assign the value for iamcs in your book], CFG, and so on.

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 (see page 16).
2. Define an import connector (see page 17).
3. Complete the Universe definition (see page 18).
4. (Optional) Customize universe tables (see page 20).
5. (Optional) Customize Workflow display settings (see page 21).

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.

4. Click Save.

   Next, you 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 *CA GovernanceMinder 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, you 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 CA GovernanceMinder 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 CA GovernanceMinder portal.

   Configuration Users Manager Field

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

   (Optional) Configuration Users Display Name Field

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

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

   Configuration Roles Manager Field

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

   (Optional) Configuration Roles Display Name Field

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

Configuration Resources Manager Field

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

(Optional) Configuration Resources Display Name Field

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

(Optional) Configuration Resources Description Field

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

(Optional) Configuration Resources Application Field

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

Note the following:

- For more information about the resource database file, see the *Programming Guide*.
- When integrating with CA Identity Manager or using the [assign the value for iamcs in your book], 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 Identity Manager, see the *Configuration Guide*.

(Optional) Approved Audit Card

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

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

(Optional) Approved alerts are

Specifies whether preapproved 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 performed on the master configuration each time an import occurs.

High Risk Threshold

Defines the value that is used to categorize high risks in a certification. A high risk has a risk score equal to or greater than this threshold value.

Default: 90

Medium Risk Threshold

Defines the value that is used to categorize medium risks in a certification. A medium risk has a risk score equal to or greater than this threshold value and less than the High Risk Threshold.

Default: 60

2. Click Save.

   Next, you can 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 21) 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) 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.

Configuring Cluster Nodes

Product: CA GovernanceMinder

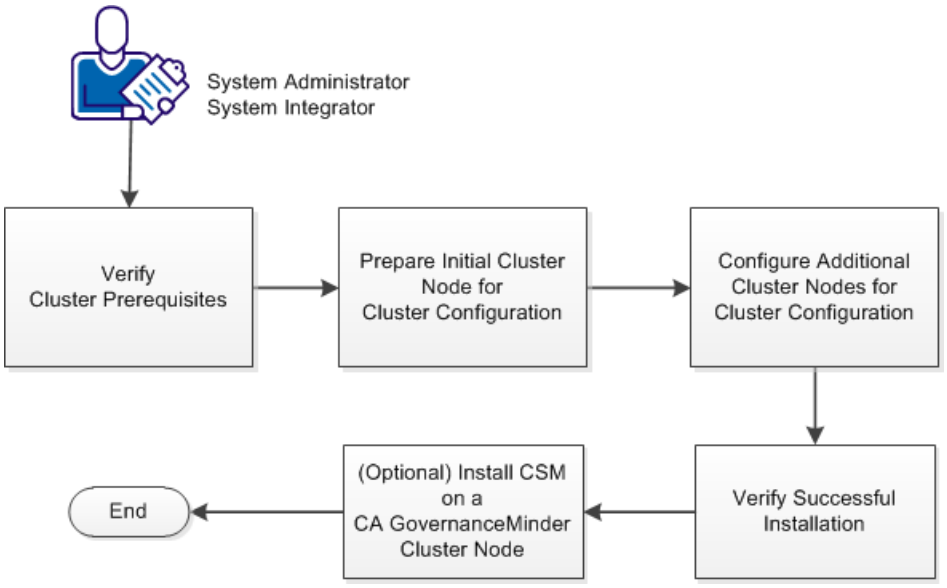
Release: 12.6.00

OS: Windows

This scenario describes how the CA GovernanceMinder administrator and system integrator prepare and configure CA GovernanceMinder cluster nodes.

How to Prepare and Configure the Cluster Nodes

The following diagram illustrates how to prepare and configure cluster nodes using the provided cluster script:



Follow these steps to prepare and configure CA GovernanceMinder cluster nodes:

1. Verify Cluster Prerequisites (see page 23).
2. Prepare initial node for cluster configuration (see page 24).
3. Configure additional nodes for cluster configuration (see page 26).
4. Verify successful installation (see page 28).
5. (Optional) Install the Connector Server Manager on a CA GovernanceMinder cluster (see page 28).

Verify Cluster Prerequisites

This section lists cluster script software prerequisites.

Verify that all the prerequisites are installed before processing cluster components. Verify that they start with no errors and then stop them.

The software prerequisites are as follows:

- CA GovernanceMinder on Node 1
- Windows or Linux operating system
- JBoss 5.1 GA (5.1.0)

- CA GovernanceMinder cluster script (extracted into a temporary work folder on Node 1)

  Note: The script is in the Core.zip file at the following location:

  `CA-RCM-12.6.00-Core\Utils&Conf\Jboss Cluster`

- Apache Ant 1.7 or higher
- An ANT_HOME environment variable on the installation server.

  Set the ANT_HOME environment variable value to the ANT installation directory.

  Example:

  ANT_HOME="C:\ant 1.7.1"

Prepare Initial Node for Cluster Configuration

You prepare the initial cluster node by defining system components, permissions, and folders to work in a cluster configuration.

Follow these steps:

1. Locate and open the prepareCluster.properties file in the temporary folder and set the following parameters:
   - CA GovernanceMinder installation directory.

     Example: CA GovernanceMinder home (Windows)

     `rcm.installation.home=C:/Program Files/CA/RCM/Server`
   - JBoss 5.1 root directory.

     Example: JBoss 5.1 root

     `jboss.5.1.home=C:/jboss-5.1.0.GA`
   - CA GovernanceMinder JBoss cluster operating system.

     Set for Windows or Linux

     Example: For Linux

     `os.provider=linux`
   - CA GovernanceMinder database. Set for MSSQL or Oracle.

     Example: For MSSQL

     `db.provider=mssql`
   - JBoss messaging database server name.

     Example:

     `db.server.name=`*`your database computer name`*

- JBoss messaging database user login.

  Example:

  `db.login.user=CA_GM_administrator`

- JBoss messaging database password login.

  Example:

  `db.login.password=your database password`

- Database port.

  Limits: 1433 MSSQL, port 1521 Oracle.

  Example:

  `db.port=1433`

- Temporary files work folder.

  Example:

  `work.dir=C:/temp/work`

- Cluster node names. A list of comma-separated host names and IP addresses.

  Example:

  `cluster.nodes=nodeA, nodeB, 3.33.333.255`

- (Oracle) Oracle server service name.

  Example:

  `oracle.service=ORCL`

2. Save and close the prepareCluster.properties file.
3. On the server where the Portal is installed, open a Command Prompt window and run the following file:

   Windows: prepareCluster.bat

   Linux: prepareCluster.sh

   This file prepares the downloaded JBoss 5.1 files to run in the cluster as Node 1.
4. Create a database and name it jboss_messaging.

   The nodes are prepared for cluster configuration. Repeat Steps 1-4 for preparing additional initial cluster nodes.

Configure Additional Nodes for Cluster Configuration

After configuring the initial node, you configure additional nodes for CA GovernanceMinder cluster configuration.

Configure additional CA GovernanceMinder cluster nodes using automatic or manual mode.

- Automatic (see page 26)
- Manual (see page 27)

Automatic Cluster Node Configuration

Automatically configure the CA GovernanceMinder cluster node. This mode configures multiple nodes using default parameters.

Follow these steps:

1. Locate and open the prepareCluster.properties file in the temporary work folder.
2. Locate the line containing the cluster.node.id=1 parameter, and set the cluster node property for this node.

   Example:

   For Node 4,

   ```
   cluster.node.id=4
   ```

   Note: The default node ID value is 1.
3. Open a Command Prompt window, and run the following file from the CA GovernanceMinder cluster work folder:

   Windows: prepareCluster.bat configure

   Linux: prepareCluster.sh configure

   This file configures JBoss 5.1 files to run as the designated node in the cluster.
4. Copy the JBoss 5.1 Home directory and all the contents from Node 1 to the next server in the cluster.
5. Repeat Steps 1-4 for each subsequent node in the cluster.

   You have automatically configured the CA GovernanceMinder cluster node.

Manual Cluster Node Configuration

Manually configure the CA GovernanceMinder cluster node. This mode is suggested for custom configurations.

Follow these steps:

1. Copy the JBoss 5.1 Home folder and all the contents from Node 1 to Node N, this server.
2. Locate and open for editing the following file in the JBoss home folder:

   Windows: eurikify.bat

   Linux: eurikify.sh
3. Assign the node to the following parameters:

   - jboss.messaging.ServerPeerID

   Defines the unique value (Node N) of this node in the cluster.

   - g

   Defines the unique cluster name.

   Example: Set the JBoss messaging peer ID and the network cluster name.

   From (default)

   ```
   run.bat -c %SERVER_NAME% -b %JBOSS_BIND_ADDRESS% -g CA_GM_Cluster -u 233.3.4.4
   -Djboss.messaging.ServerPeerID=1  %*
   ```

   To (assigned node number)

   ```
   run.bat -c %SERVER_NAME% -b %JBOSS_BIND_ADDRESS% -g CA_GM_Cluster -u 233.3.4.4
   -Djboss.messaging.ServerPeerID=2  %*
   ```
4. Save and close the file.
5. Open the server.xml file located in the following folder:

   JBoss 5.1 Home/server/all/deploy/jbossweb.sar/

   a. Locate and replace the following text:

   ```
   <Engine name="jboss.web" defaultHost="localhost">
   ```

   With

   ```
   <Engine name="jboss.web" defaultHost="localhost"
   jvmRoute="worker-node-name">
   ```

   Note: "*worker-node-name*" is the load balancer worker node name.

   b. Save and close the server.xml file.

   You have manually configured the CA GovernanceMinder cluster node.

Verify Successful Installation

When the installation is successful, you can access the CA GovernanceMinder Portal.

Follow these steps:

1. Open a Command Prompt window on Node 1, navigate to the JBoss home folder and run the following file:

   Windows: eurikify.bat

   Linux: eurikify.sh

   The CA GovernanceMinder and JBoss servers on Node 1 starts.

2. Review the logs and ensure Node 1 starts with no error messages.

   The CA GovernanceMinder cluster node log folder is:

   jboss.5.1home\server\all\log

   Note: *jboss.5.1home* is the CA GovernanceMinder cluster node home directory.

3. Stop the CA GovernanceMinder and JBoss servers on Node 1.

   You have verified the CA GovernanceMinder installation.

(Optional) Install the Connector Server Manager on a CA GovernanceMinder Cluster Node

Use the CSM to manage the Java Connector Server (JCS). The JCS enables you to connect to and manage endpoints. CA GovernanceMinder can connect to a standalone JCS and automatically import and export data from a single endpoint.

Note: Install CSM on one cluster node only.

Follow these steps:

1. Install CA GovernanceMinder on a JBoss clustered node.

   Note: Do **not** select to install CSM while installing CA GovernanceMinder.

2. Create a CSM work forder on the clustered node and copy the complete JBoss 5.1 GA folder and all its contents.

   Example (Windows):

   `C:\Program Files\CA\RCM\Server\Connector Server Management\JBoss5.1GA_CSM`

3. From the CA GovernanceMinder installation folder, run the CSM installer and install CSM in the JBoss folder as defined in Step 2.

   Note: Specify port 8280 for the CSM when you install with the CSM installer.

4. Add the JBoss service binding parameter.

   Windows:

   a. Go to Start, Programs, CA, Connector Server Manager, and right-click Start Connector Server Management.

   b. Select the Properties option, and select the Shortcut tab.

   c. Add the following parameter to the Start Connector Server Management Server command line:

      ```
      -Djboss.service.binding.set=ports-02
      ```

      Example:

      From

      ```
      C:\jboss-5.1.0.GACSM\bin\run.bat -c default
      ```

      To

      ```
      C:\jboss-5.1.0.GACSM\bin\run.bat -c default
      -Djboss.service.binding.set=ports-02
      ```

   Linux:

      Use the following command to run JBoss:

      ```
      C:\jboss-5.1.0.GACSM\bin\run.sh -c default
      -Djboss.service.binding.sets=ports-02
      ```

   The JBoss service binding parameter is added.

5. Navigate to the following folder to locate the sajcsui_environment.properties.xml:

   CSM JBOSS DIR\server\eurekify\deploy\iam_csm.ear\user_console.war\META-INF

6. Open the sajcsui_environment.properties.xml file and add the following parameter:

   AuthenticationWebService="@http://*YourComputerName*:8280/eurekify/services/ssoService"

   Where *YourComputerName* is the name of the current server.

7. Save and close the sajcsui_environment.properties.xml file.

8. Start CA GovernanceMinder, and in the Portal modify the following CA GovernanceMinder properties accordingly:

   - sso.sajcsui.enabled=true
   - sso.sajcsui.url=http://CSM_MACHINE_NAME:8280/iam/csm/csmanage/
   - sso.sajcsui.predefinedUser=CSM_PASSWORD

   You have installed CSM on a CA GovernanceMinder JBoss cluster node.

Configuring Reporting

Product: CA GovernanceMinder

Release: 12.6.00

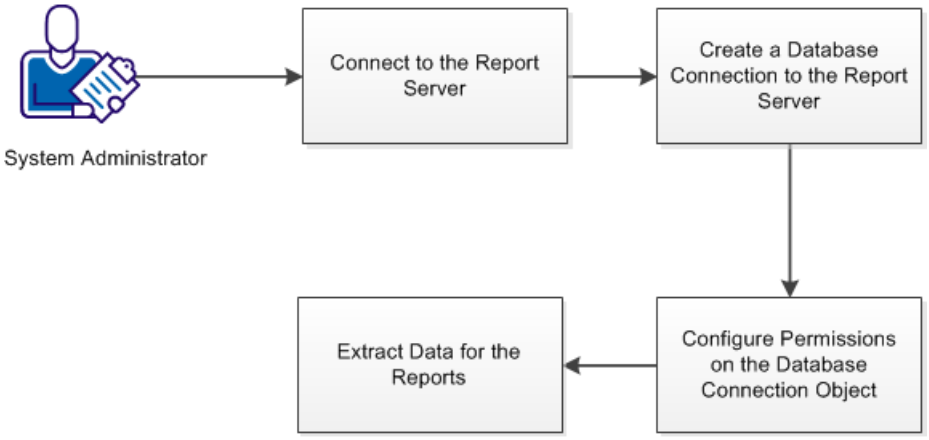
OS: Windows

This scenario describes how the CA GovernanceMinder system administrator configures reporting.

Chapter 4: How to Configure Reporting

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

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



Follow these steps:

1. Connect to the report server (see page 32).
2. Create a database connection to the report server (see page 32).
3. Configure permissions on the database connection object (see page 33).
4. Extract data for the reports (see page 34).

Connect to the Report Server

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

Follow these steps:

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

   The BusinessObjects checkup screen appears.

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

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

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

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

Create a Database Connection to the Report Server

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

Follow these steps:

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

      The Universe Parameters screen appears.

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

c. Enter a connection name and select a driver as follows:

- Microsoft SQL 2005 or 2008: OLE DB Providers
- Oracle 10 or 11: Oracle Client

d. Provide database credentials.

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

f. Click OK.

The Universe Parameters screen closes.

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

a. Go to File, and click Save.

b. Go to File, Export.

c. Click OK.

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

Configure Permissions on the Connection Object

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

Follow these steps:

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

   http://*businessobjects_hostname*:8080/CmcApp

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

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

Extract Data for Reports and Dashboards

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

Follow these steps:

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

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

Configuring a [assign the value for cabi in your book] Server

Product: CA GovernanceMinder

Release: 12.6.02

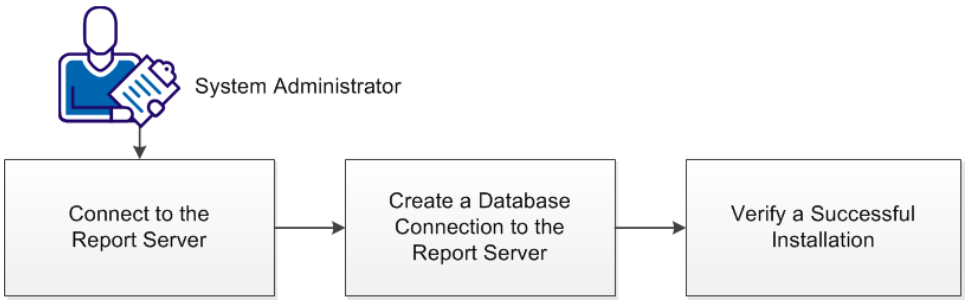
OS: Windows

This scenario describes how a system administrator configures CA GovernanceMinder with a [assign the value for cabi in your book] Server.

Chapter 5: How to Configure a [assign the value for cabi in your book] Server

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

Important! For this release, install CA Business Intelligence 3.3 as the reporting engine. (BusinessObjects XI 3.1 SP5) For more information about installing [assign the value for cabi in your book] 3.3, see the [assign the value for cabi in your book] documentation.



Follow these steps:

1. Connect to the Report Server (see page 35).
2. Create a Database Connection to the Report Server (see page 36).
3. Verify a successful installation (see page 37).

Connect to the Report Server and Deploy Reports

To integrate the product with [assign the value for cabi in your book], connect to the report server, and deploy reports.

Follow these steps:

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

   The BusinessObjects checkup screen appears.

2. Enter the report server credentials in this screen. The following credential is not self-explanatory:

   InfoView URL

   Defines the Business Object InfoView URL address.

   Default: http://localhost:8080/InfoViewApp/logon/logoff.do

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

3. Click Start to load the BIAR file.

   The BIAR file contains all the product default reports.

   You have connected to the report server and deployed default reports.

Create a Database Connection to the Report Server

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

Follow these steps:

1. On the [assign the value for cabi in your book] server, import a CA GovernanceMinder universe as follows:

   a. Go to Start, Programs, BusinessObjects XI 3.1, Business Objects Enterprise, Designer.

      The Universe Designer appears.

   b. Go to File, Import.

      The Import Universe window appears.

   c. In the Folder field, select CA GovernanceMinder, select Open the selected universes, and click OK.

      The universe is selected, successfully imported, and displays.

2. In the Designer Tool, create a connection to your database.

   a. Go to File, Parameters.

      The Universe Parameters window appears.

   b. Click the Definition tab, and click New.

      The New Connection Wizard screen appears.

c. Click Next, and in the Database Middleware Selection screen, add a Connection Name.

d. Select a connector from the displayed list, and click Next.

The Login Parameters screen appears.

e. Enter the credentials to access your database using JDBC middleware, and click Test Connection.

f. Click Next and Finish.

You have created and tested a connection to the I2 database.

3. Save the file and export the changes to the report server as follows:

a. Go to File, Save.

b. Go to File, Export.

The Export Universe window appears.

c. Select the domain and universe and click OK.

You have successfully saved and exported the universe.

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

Verify a Successful Installation

Verify that the [assign the value for cabi in your book] server is correctly connected by creating and viewing a report.

[assign the value for cabi in your book] reports are available for universes where you run the ETL process.

Example: View a certification report

This example describes how to generate and view a certification report.

Follow these steps:

1. Create a certification in a universe.
2. Run ETL for the selected universe.

a. In the Portal, go to Administration, Manage the ETL process.

b. Select a universe and click Run ETL.

Data from the selected universe is processed for reporting, and the ETL process completes.

3. In the Portal, go to Reports, View Reports.

The View Reports screen appears.

a. Select a universe, and click Certification as a report type from the available list.

   A new browser window with report prompts displays.

b. Select the mandatory fields, move the values that appear in the table from the left to the right side of the window, and click Run Query.

   The data is processed and the report displays.

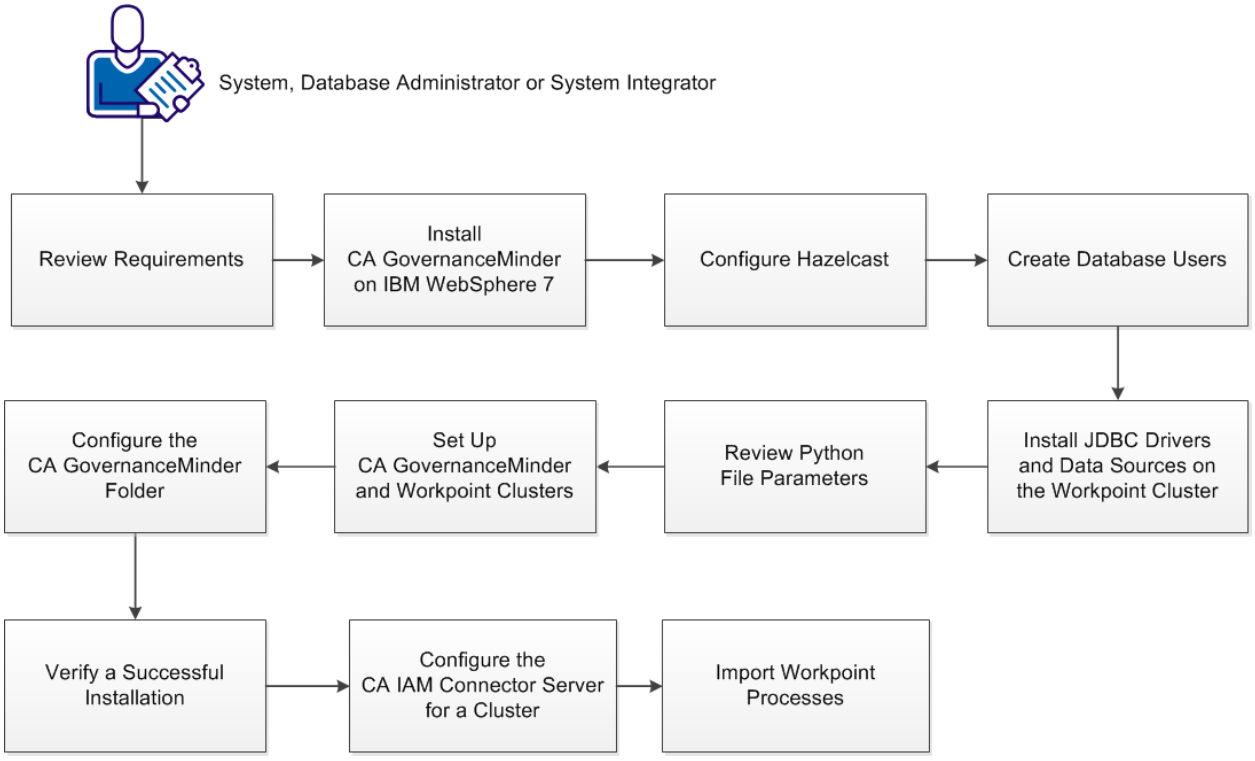
You have verified that the [assign the value for cabi in your book] server is correctly connected.

Chapter 6: How to Install CA GovernanceMinder on an IBM WebSphere Cluster

As a system database administrator or system integrator, you install CA GovernanceMinder with IBM WebSphere Application Server (WAS) 7 on Red Hat Enterprise Linux (RHEL) 6.2.

The supplied script installs CA GovernanceMinder and WebSphere by automating various installation tasks. WebSphere is an application server that provides application delivery with operational efficiency, reliability, security, and control. Clustering increases computer processing power, load balancing, and provides application high availability.

The following diagram illustrates how to install CA GovernanceMinder and WebSphere with the supplied script:



Follow these steps:

1. Review requirements (see page 40).
2. Install CA GovernanceMinder on IBM WebSphere 7 (see page 41).

3. Configure Hazelcast (see page 43).
4. Create database users (see page 44).
5. Install JDBC drivers and data sources on the Workpoint cluster (see page 45).
6. Review Python file parameters (see page 48).
7. Set up CA GovernanceMinder and Workpoint clusters (see page 49).
8. Configure the CA GovernanceMinder folder (see page 49).
9. Verify a successful installation (see page 50).
10. Configure the [assign the value for iamcs in your book] for a cluster (see page 51).
11. Import Workpoint processes (see page 51).

Review Requirements

When you install the product on IBM WebSphere on Red Hat Enterprise Linux (RHEL) 6.2, consider the following requirements.

- **IBM WebSphere 7.0 Network Deployment Application Server**—Install the IBM WebSphere 7.0 Network Deployment Application Server.

  Important! When running the setup script, select the Cell (deployment manager and a managed node) option.

- **Java Development Kit (JDK)**—CA GovernanceMinder 12.6.1 requires Oracle Java SE Development Kit 6u45 (1.6_45). For a list of supported JDKs, see the Platform Support Matrix available at CA Technologies Support Online.

  Note: When using a 64-bit JDK, and available memory is greater than 1400M (default), set the JVM maximum setting at 4 GB

- **Verify that the following packages exist in this order:**
  - glibc-2.12-1.25.el6.i686.rpm
  - libX11-1.3-2.el6.i686.rpm
  - libxcb-1.5-1.el6.i686.rpm
  - libXtst-1.0.99.2-3.el6.i686.rpm
  - libXau-1.0.5-1.el6.i686.rpm
  - libXi-1.3-3.el6.i686.rpm

- libXext-1.1-3.el6.i686.rpm
- nss-softokn-freebl-3.12.9-3.el6.i686.rpm
- dos2unix-3.1-37.el6.x86_64.rpm

- **Run Commands**—Run the following command to improve performance (Entropy):
  `rm /dev/random && mknod -m 644 /dev/random c 1 9`
- **Java Virtual Machine (JVM) 1.6.0**—Install JVM 1.6.0, and set the following java environment variables:
  - JAVA_HOME=/usr/java/jdk1.6.0_20/
  - PATH=$PATH:/usr/java/jdk1.6.0_20/bin

Note: For more information about installation prerequisites, see the *Installation Guide*.

Install CA GovernanceMinder on IBM WebSphere 7

This procedure describes how you install the CA GovernanceMinder server in a WebSphere environment. You must install the product as a root user on the same system where you have installed IBM WebSphere Network Deployment. The installer also installs and configures CA GovernanceMinder databases and data tables on a specified SQL or Oracle database server.

Follow these steps:

1. Verify that the SQL or Oracle server that is determined to host your databases is running.
2. Do the following:
   a. Download and install the latest Oracle JDK 1.6.X from the Oracle website.

      Note: We recommend that you download any Oracle JDK version above 1.6.23.

   b. Configure the Red Hat Enterprise Linux 6.2 Java alternatives.

      For example, run the following commands from the command prompt:

      ```
      /usr/sbin/alternatives --install  /usr/bin/java java
      /usr/java/jdk1.6.0_45/bin/java 1500
      ```

      ```
      /usr/sbin/alternatives --config java
      ```

      Note: In this example, the JDK installation root is as follows:

      ```
      /usr/java/jdk1.6.0_45
      ```

   c. Verify that the default Java command is now the Oracle JDK 6.45.

      From the command prompt, enter in the following command:

      ```
      java -version
      ```

      The Java version displays the following information:

      ```
      java version "1.6.0_45"
      ```

   d. Set the following java environment variables to the CA GovernanceMinder and IBM WebSphere cluster node installation:

      ```
      JAVA_HOME=JDK_6_install_root
      ```

      For example, add the following lines to the /root/.bashrc file:

      ```
      JAVA_HOME=/usr/java/jdk1.6.0_45
      ```

      ```
      export JAVA_HOME
      ```

      Note: You only set the environment variables on the node where you install CA GovernanceMinder, and not every node.

   You have configured Red Hat E Enterprise Linux 6.2 Java alternatives, verified default commands, and set Java environment variables.
3. Run the InstCARCM.bin installation program from the installation files.

   The CA GovernanceMinder installer opens.
4. Select the language that you want for the Portal, and click OK.

   Note: The language that you select affects the Portal interface only and not the installation or any other component.

5. Complete the installer by providing the necessary information. The following options are not self-explanatory:

   Application Server

   Specifies WebSphere: Prepare '.ear' installation files.

   Workpoint Server Host

   Specify *one* of the following server options:

   - This server - You install the Workpoint server on the CA GovernanceMinder server.
   - Remote server - Specify a remote Workpoint server.

6. Review your installation choices, and click Install.

   The installer runs the customized installation package.

7. When the installation completes, click Done to close the installer.

   You have installed CA GovernanceMinder and selected WebSphere as the application server in the Application Server step.

Next, you configure Hazelcast.

Configure Hazelcast

This procedure describes how to configure Hazelcast. Hazelcast is an open source clustering and highly scalable Java data distribution operating environment that CA GovernanceMinder uses.

For the CA GovernanceMinder cluster integration, edit the hazelcast.xml file to adjust the Hazelcast lock mechanism. The Hazelcast.xml file is located in the eurekify.war file.

Follow these steps:

1. Locate the hazelcast.xml file in the following folder:

   `eurekify.ear/eurekify.war/WEB-INF/classes`

   Note: Extract the eurekify.ear file before deploying to the cluster.

2. Open the hazelcast.xml file in an editor and locate the following group element:

   ```
   < group>
      <name>dev_RCM_WAS</name>
      <password>dev-pass</password>
   </group>
   ```

3. To match a unique name for your CA GovernanceMinder cluster, edit this element.

4. Locate the following element:
```
<tcp-ip enabled="true">
  <interface>127.0.0.1</interface>
</tcp-ip>
```
5. Add all your cluster member host names to the element as in Step 4.

   For example, the element would read as follows:
```
<tcp-ip enabled="true">
   <interface>Server1</interface>
   <interface>Server2</interface>
   <interface>Server3</interface>
   <interface>Server4</interface>
</tcp-ip>
```
6. Save the changes to the hazelcast.xml file and exit.

   You have configured the hazelcast.xml file to adjust the Hazelcast lock.

Next, you create database users to synchronize Java Messaging Service (JMS) topics.

Create Database Users

This procedure describes how to create database users to synchronize Java Messaging Service (JMS) topics.

Follow these steps:

1. Create the following database users:
   - gvmBus
   - wpBus
2. (Oracle only) Verify that the databases have the appropriate permissions by running the following SQL commands as user sys:
```
grant select on pending_trans$ to WPDS;
grant select on dba_2pc_pending to WPDS;
grant select on dba_pending_transactions to WPDS;
```
   - (if using an Oracle JDBC 10.2.0.3 or lower driver):
```
grant execute on dbms_system to WPDS;
```
   - (if using an Oracle JDBC 10.2.0.4 or higher driver):
```
grant execute on dbms_xa to WPDS;
```
3. (Oracle only) Restart the Oracle server.

   You have created database users to synchronize Java Messaging Service (JMS) topics.

Next, you install Server JDBC drivers and data sources on the Workpoint cluster.

Install JDBC Drivers and Data Sources on the Workpoint Cluster

This procedure describes how to install JDBC API support server cluster connections to the Microsoft and Oracle SQL database.

- **Microsoft:** (http://www.microsoft.com/en-us/download/default.aspx) XA data sources with Microsoft Distributed Transaction Coordinator (MS DTC) manage distributed transactions. To enable a specific user to participate in distributed transactions with the JDBC driver, assign the SqlJDBCXAUser role on the master database to the user that you create for the WDPDS database.
- **Oracle:** (http://www.oracle.com/technetwork/indexes/downloads/index.html) When an Oracle database server hosts CA GovernanceMinder databases, install JDBC drivers on the WebSphere Application Server. XA data sources manage distributed transactions. To enable a specific user to participate in distributed transactions with the JDBC driver, assign the SqlJDBCXAUser role on the master database to the user that you create for the WDPDS database.

Next, you review Python file parameters.

Install Microsoft SQL Server JDBC Drivers and Data Sources on the Workpoint Cluster

Valid on Microsoft SQL Server.

This procedure describes how you install Microsoft SQL Server JDBC drivers and data sources on the Workpoint cluster.

Java applications use the JDBC XA driver to establish concurrent connections to multiple databases through their associated resource managers.

Install the JDBC XA drivers on all SQL servers, and on the WebSphere application server.

Note the following:

- With a 32-bit SQL server, use the sqljdbc_xa.dll file in the x86 folder, even if the SQL server is installed on an x64 processor.
- With a 64-bit SQL server on the x64 processor, use the sqljdbc_xa.dll file in the x64 folder.
- With a 64-bit SQL server on an IA-64 processor, use the sqljdbc_xa.dll file in the IA64 folder.

Follow these steps:

1. Install the Microsoft SQL JDBC installer on the SQL server.

   Download the installer, Microsoft JDBC Driver for SQL (sqljdbc_4.0.2206.100_enu.exe), from the Microsoft Download Center.

2. Enable the XA transactions on the SQL server as follows:

   a. In the computer where you install the SQL server, browse to the Control Panel.

   b. Click Administrative Tools, Component Services.

   c. Right-click My Computer and click Properties.

   d. Click the MSDTC tab and click Security Configuration.

   e. Select Enable XA Transactions.

   f. Save the changes and restart the SQL server.

3. Copy and install drivers on other SQL cluster servers as follows:

   a. Locate the JDBC distributed transaction components under the \xa folder of the JDBC driver installation directory.

   b. Copy the file sqljdbc_xa.dll.

   c. Paste this file in the following directory of every SQL server computer that participates in distributed transactions:

      ```
      %SQL_SERVER_INSTALL%\Binn
      ```

   d. Execute the database script xa_install.sql on every SQL server instance that participates in distributed transactions. This script installs sqljdbc_xa.dll as an extended stored procedure.

      Note: When you run this script, log in as an administrator for the SQL Server instance.

4. Install the drivers on WebSphere as follows.

   a. In the original JDBC installation folder on the SQL server, locate the sqldbc.jar file in the following directory:

      `Microsoft SQL Server 2005 JDBC Driver\sqljdbc_1.2\enu`

   b. Copy this file to the WebSphere application server under the following directory:

      `WAS_install_root``/essentials/JDBC/`

      Note: *WAS_install_root* is the WebSphere Application Server installation directory.

5. To implement the new data source definitions, restart the WebSphere Application Server or the Deployment Manager service as required in your WebSphere environment.

   You have installed the Microsoft SQL Server JDBC drivers and data sources on the Workpoint cluster.

Install Oracle JDBC Drivers and Data Sources on the Workpoint Cluster

Valid on Oracle database.

This procedure describes how you install Oracle JDBC drivers and data sources on the Workpoint cluster.

Follow these steps:

1. Download the ojdbc14.jar file from the Oracle Download Center to the WebSphere application server, and place the file under the following directory:

   `WAS_install_root``/essentials/JDBC/`

   Note: *WAS_install_root* is the WebSphere application server installation directory.

2. In the WebSphere administration console, click Resources, JDBC, JDBC Providers and create a JDBC provider with the following settings:

   - The server provider:

     Name: ServerProvider

     Provider Type: Oracle JDBC Driver

     Implementation Type: data source

- The server XA provider:

  Name: ServerXAProvider

  Provider Type: Oracle JDBC Driver (XA)

  Implementation Type: XA data source

- Apply the following settings to both JDBC providers:

  Scope – Workpoint_cluster

  Database type – Oracle

  Class path – *WAS_install_root*/essentials/JDBC/ojdbc14.jar

3. Restart the WebSphere Application Server or the Deployment Manager service as required in your WebSphere environment.

   The new data source definitions are implemented.

   You have installed the Oracle JDBC drivers and data sources on the Workpoint cluster.

Review Python File Parameters

This procedure describes how you review the Python file to verify correct CA GovernanceMinder installation paths and data sources, and retain reusable memory. You download this file with the CA GovernanceMinder installation files. This file contains classes that can be used as reusable data sources and can construct dictionaries from other mappings or sequences of pairs.

Follow these steps:

1. Locate and open the dataSources.py file in the following folder:

   gm_install/rcm-websphere/WAS-Scripts

2. Change the passwords for the gvmBus and the wpBus users to the passwords set during the creation.

3. Save the dataSources.py file.

   You have reviewed the Python file.

Next, you set up the CA GovernanceMinder and Workpoint clusters.

Set Up CA GovernanceMinder and Workpoint Clusters

This procedure describes how you set up CA GovernanceMinder and Workpoint clusters on WebSphere.

Follow these steps:

1. Navigate to the following directory:

   gm_install\rcm-websphere\WAS-Scripts

2. Open a Command Prompt and enter the following command:

   ./DeployGVM.sh /opt/IBM/WebSphere/AppServer/bin

   This command instructs the installation script where to place the installation files.

   You have set up CA GovernanceMinder and the Workpoint clusters on WebSphere.

Next, you configure the CA GovernanceMinder folder to configure and copy essential files to the cluster nodes.

Configure the CA GovernanceMinder Folder

This procedure describes how you configure the CA GovernanceMinder installation folder to set up and copy essential files to the cluster nodes.

Follow these steps:

1. Locate and copy the *GM_Install_Dir* folder to the WebSphere clustered node server.
2. Change the directory as follows:

   GM_Install_Dir\rcm-websphere\WAS-Scripts

3. Locate and run the setupEssentials.py file from the following folder:

   WAS_HOME\profiles*NODE_NAME*\bin\wsadmin.bat -lang jython -f setupEssentials.py

4. Repeat Steps 1, 2 and 3 for each cluster node.

   You have configured the CA GovernanceMinder installation folder to configure and copy essential files to the cluster nodes.

Next, verify a successful installation.

Verify a Successful Installation

This procedure describes how you verify a successful installation after you complete installing the product. When the CA GovernanceMinder installation is successful, you can access the CA GovernanceMinder Portal.

Follow these steps:

1. Select and start one server from the CA GovernanceMinder cluster, CA GovernanceMinder, and installed applications, including reports.
2. Review the started server logs and verify that no log errors exist.
3. Start all other servers in the CA GovernanceMinder cluster.
4. Review all the product cluster logs and verify that no errors exist in the logs.

   You can access the Portal after a successful installation.
5. Open a browser and enter the following URL:

   `http://serverhost:port/eurekify/portal/login`

   Note: *serverhost:port* is the network address and communications port of the CA GovernanceMinder server or load balancer. The WebSphere/AIX server default port is 9080.

   The CA GovernanceMinder Portal login page appears.
6. Log in using the following default administration credentials:
   - **Username:** AD1\EAdmin
   - **Password:** eurekify

   The Portal home page appears.
7. Set your Properties and Common properties URL setting under Administration, Settings.
8. Navigate to Reports, Configuration Reports, and select Configuration Properties.
9. Select ConfigWithRoles to verify that the report application is working.

   You have verified a successful installation.
10. (Upgrade only) Clear the browser cache or refresh the web page to replace old graphical elements.

Next, configure the [assign the value for iamcs in your book] for a cluster.

Configuring the [assign the value for iamcs in your book] for a Cluster

You configure the [assign the value for iamcs in your book] for a cluster after the installation completes. When you install the [assign the value for iamcs in your book] in a cluster environment, install the [assign the value for iamcs in your book] on one of the nodes, or on a dedicated node.

After the installation, edit the following properties to reflect the location of the [assign the value for iamcs in your book]:

- jcs.ui.url=*IAMCS_hostname*

  This name is the [assign the value for iamcs in your book]hostname of the computer where the [assign the value for iamcs in your book] is installed.

- jcs.ui.enabled=true
- jcs.ui.username=*username*

  Default: admin

- jcs.ui.password=*IAMCS_password*

  The [assign the value for iamcs in your book] password is the one provided during the installation.

Next, you import the Workpoint processes to enable certification campaigns and other business processes.

Import Workpoint Processes

This procedure describes how you import Workpoint processes. To enable certification campaigns and other business processes, import predefined workflow processes into Workpoint.

Follow these steps:

1. Verify that the CA GovernanceMinder cluster is running.
2. Log in to the Portal as an administrator.

   The Portal home page appears.

3. Go to Administration, Settings, and click Workpoint DB Administration.

   The Workpoint DB Administration screen appears.

4. Under Update Workpoint Processes, verify the CA GovernanceMinder Server Host Name, Port, and HTTPS setting.

   Note: In a clustered environment, enter the CA GovernanceMinder (load balancer) name instead of the server hostname.

5. Click Update.

   The product populates the Workpoint database with predefined Workpoint processes and related data.

You have enabled certification campaigns and other business processes, and imported predefined workflow processes into Workpoint.

You have completed the CA GovernanceMinder on IBM WebSphere 7 installation process.

Installing CA GovernanceMinder and Oracle Real Application Clusters (RAC)

This scenario describes how to install CA GovernanceMinder with Oracle Real Application Clusters (RAC).

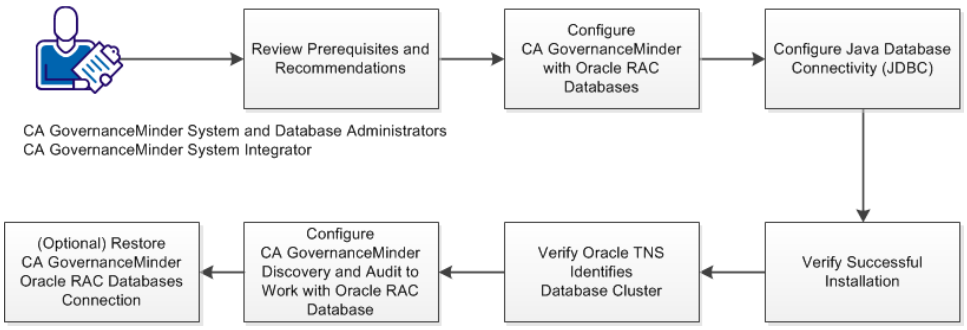
This scenario targets the following CA GovernanceMinder users:

- System and database administrators
- System integrators

How to Install CA GovernanceMinder and Oracle RAC

You configure CA GovernanceMinder to function in an Oracle RAC environment. Oracle RAC provides clustering and high availability software for Oracle database environments.

The following diagram illustrates how to install CA GovernanceMinder with Oracle RAC databases:



Follow these steps to install CA GovernanceMinder with Oracle RAC databases:

1. Review prerequisites and recommendations (see page 53).
2. Configure CA GovernanceMinder with Oracle RAC databases (see page 53).
3. Configure Java Database Connectivity (JDBC) (see page 57).
4. Verify successful installation (see page 58).
5. Verify Oracle TNS Identifies Database Cluster (see page 59).
6. Integrate CA GovernanceMinder Discovery and Audit with Oracle RAC databases (see page 60).
7. (Optional) Restore CA GovernanceMinder Oracle RAC databases connection (see page 62).

Review CA GovernanceMinder and Oracle RAC Prerequisites

This section lists CA GovernanceMinder and Oracle RAC prerequisites.

- CA GovernanceMinder databases must use UTF-8 (AL32UTF8) encoding.
- We recommend enabling 400 connections for each CA GovernanceMinder server that is connected to the same database, even if they are connected to different schemas.
- We recommend that you expand the CA GovernanceMinder cache memory limits to support considerable CA GovernanceMinder configurations. The default setting limits the memory cache to 500,000 elements. We recommend that you reset the CA GovernanceMinder cache limits to 900,000 elements.

Configure CA GovernanceMinder with Oracle RAC Databases

You configure CA GovernanceMinder with Oracle RAC databases by adding roles, establishing communication, and defining parameters.

Follow these steps:

1. Create a CA GovernanceMinder database user (schema). This user must have the following permissions and settings:
   - Roles: CONNECT, RESOURCE
   - System Privileges: ALTER SESSION, CREATE CLUSTER, CREATE DATABASE LINK, CREATE SEQUENCE, CREATE SESSION, CREATE SYNONYM, CREATE TABLE, CREATE VIEW, CREATE CLUSTER, CREATE INDEXTYPE, CREATE OPERATOR, CREATE PROCEDURE, CREATE SEQUENCE, CREATE TABLE, CREATE TRIGGER, CREATE TYPE, SELECT ANY DICTIONARY

   The CONNECT role provides the create session permission. The RESOURCE role provides several create system privileges, and provides for previous Oracle database compatibility releases.

2. Edit the tnsnames.ora file for the database cluster from the database server.

   You modify the tnsnames.ora file by adding your cluster address and port. The Oracle client uses the tnsnames.ora file to connect to the Oracle server. Do the following:

   a. Locate the tnsnames.ora file in the Oracle home directory. The tnsnames.ora file is located in the following folder:
   Oracle_home/NETWORK/ADMIN

   b. Locate the instances that define your clustered service and add your cluster address and port.

   Example:

```
RCMDB1 =
   (DESCRIPTION =
     (ADDRESS = (PROTOCOL = TCP)(HOST = oraclusternode1-vip)(PORT = 1521))
     (ADDRESS = (PROTOCOL = TCP)(HOST = oraclusternode2-vip)(PORT = 1521))
     (LOAD_BALANCE = yes)
     (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = RCMDB1
   )
)
```

   In this example, your Oracle RAC cluster and port have been defined.

   c. Save and close the file.

   The tnsnames.ora file is edited.

3. Update the hosts file to define current cluster nodes.

   You define the IP addresses and the Oracle RAC host names. Do the following:

   a. Locate the hosts file in the following folder:

      gm_install/Windows/System32/drivers/etc

   b. Define the IP addresses and the Oracle RAC host names.

   c. Save and close the file.

      You have updated the hosts file to define the current cluster nodes.

      Example: In this example, in the # RAC VIRTUAL INTERFACES section, IP address 10.0.0.82 is defined as rac1-vip.localdomain, and IP address 10.0.0.83 is defined as rac2-vip.localdomain.

      ```
      ##########################################
      # Do not remove the following line, or various programs
      # that require network functionality will fail.
      127.0.0.1       localhost.localdomain localhost
      10.0.0.39       ca_gm_linux46.localdomain   ca_gm_linux46
      # RAC VIRTUAL INTERFACES
      10.0.0.82       rac1-vip.localdomain    rac1-vip
      10.0.0.83       rac2-vip.localdomain    rac2-vip
      # RAC PUBLIC INTERFACES
      10.0.0.182      rac1.localdomain        rac1
      10.0.0.183      rac2.localdomain        rac2
      ##########################################
      ```

4. Edit the eurekify.properties file to define the database host name as the CA GovernanceMinder SDB database. The SDB contains CA GovernanceMinder Master and Model data.

   Important! When you upgrade from CA GovernanceMinder 12.5 SPx with Oracle RAC, edit this property file after the upgrade process completes.

   a. Locate the eurekify.properties file in the following folder:

      gm_install/Program Files/CA/RCM/Server/eurekify-jboss/conf/

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

b. Add the following property:

```
sdb.host=RCMDB1
```

Note: *RCMDB1* is the Oracle RAC database service name as defined above.

c. Save and close the file.

You have edited the eurekify.properties file to define the database host name as the CA GovernanceMinder SDB database.

Note: Update this property file in each node when you configure CA GovernanceMinder to work in a cluster.

5. Run the CA GovernanceMinder installer, and in the database parameters section, define the following database parameters:

- **Oracle Server Host** - The IP address of one of the cluster nodes.
- **Oracle Service name** - Cluster Database service name (not the nodes).

Example:

```
Specify Oracle SQL Server Information

Oracle Server Host (DEFAULT: rcmlinux46.localdomain): rac1

Oracle Service Name (DEFAULT: ORCL): RCMDB1

Specify Oracle Server port (DEFAULT: 1521):1521
```

Note: For more information, refer to the *CA GovernanceMinder Installation Guide*.

6. Increase the database sessions and processes parameters from the default setting to reduce exceptions.

a. Connect to the database with the system account.

b. Run the following commands:

```
alter system set sessions=400 scope=spfile;

alter system set processes=400 scope=spfile;
```

c. Restart the entire database (all cluster instances).

Database sessions and process parameters are increased.

You have configured CA GovernanceMinder with Oracle RAC databases. You now configure JDBC connectivity.

Configure Java Database Connectivity (JDBC)

You configure the JDBC to connect to a database and increase default cache settings. JDBC, an API for the Java programming language, defines how a client accesses a database by providing querying methods and updating database data.

Follow these steps:

1. Backup the eurekify-ds.xml and wp-ds.xml files from the following folder:

   gm_install/CA/RCM/Server/eurekify-jboss/server/eurekify/deploy/

2. Update JDBC URL values to define Oracle RAC database cluster rac1-vip and rac2-vip. Do the following:

   a. Locate the following elements in both files:

      ```
      <connection-url>jdbc:oracle:thin:@rac:1521/RCMDB1</connection-url>
      ```

   b. Replace with the following text that defines the JDBC URL to Oracle RAC cluster rac1-vip and rac2-vip databases:

      ```
      <connection-url>jdbc:oracle:thin:@(DESCRIPTION=(LOAD_BALANCE=on)
      (ADDRESS=(PROTOCOL=TCP)(HOST=rac1-vip.localdomain) (PORT=1521))
      (ADDRESS=(PROTOCOL=TCP)(HOST=rac2-vip.localdomain) (PORT=1521))
      (CONNECT_DATA=(SERVICE_NAME=RCMDB1)))</connection-url>
      ```

   c. Save and close the files.

      The JDBC URL values define Oracle RAC database cluster rac1-vip and rac2-vip.

3. Reset the CA GovernanceMinder cache limits, as follows:
   a. 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
   b. 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.
   c. Save and close the file.

      The CA GovernanceMinder cache limits are reset.

      You have configured the JDBC. You now verify a successful CA GovernanceMinder installation.

Verify Successful Installation

When the installation is successful, you can access the CA GovernanceMinder portal.

Follow these steps:

1. Select one server from the CA GovernanceMinder Oracle RAC cluster and start it.
2. Review the logs and ensure that the CA GovernanceMinder Oracle RAC starts with no error messages.

   The CA GovernanceMinder cluster node log folder is:

   *gm_install/server/all/*log

   Note: *gm_install* is the CA GovernanceMinder home directory.
3. Start all other servers in the CA GovernanceMinder Oracle RAC cluster.
4. Review all CA GovernanceMinder cluster logs and verify that no errors exist in the logs.

5. Open a browser and enter the following URL:

   `http://serverhost:port/eurekify/portal/login`

   Example: http://CA_GM_OracleRAC_01:8080/eurekify/portal/login

   The CA GovernanceMinder portal login page appears.

6. Log in using the default administration credentials:

   - **Username:** AD1\EAdmin
   - **Password:** eurekify

   Note: The password can be any password. It must be at least one character. The field must not be blank.

   The portal home page appears.

   You have verified a successful CA GovernanceMinder Oracle RAC database installation. You now verify that Oracle TNS identifies the database cluster.

Verify Oracle TNS Identifies Database Cluster

You verify that the Oracle TNS entries in the tnsnames.ora file identify your Oracle RAC database structure. Oracle Transparent Network Substrate (TNS) provides a network platform of different protocols to function as a homogeneous network. The tnsnames.ora file is a configuration file that defines database addresses by establishing connections to them.

Follow these steps:

1. Locate the tnsnames.ora file on the computer hosting the CA GovernanceMinder Discovery and Audit tool.

   The tnsnames.ora file is located in the following folder:

   `Oracle_home/NETWORK/ADMIN`

2. Open the tnsnames.ora file and verify that the existence of TNS entries identifies your database cluster.

   Example:

```
RCMDB1 =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = rac1-vip.localdomain)(PORT = 1521))
    (ADDRESS = (PROTOCOL = TCP)(HOST = rac2-vip.localdomain)(PORT = 1521))
    (LOAD_BALANCE = yes)
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = RCMDB1)
    )
  )
```

3. Save and close the file.

   You have verified that the Oracle TNS entries in the tnsnames.ora file identify your Oracle RAC database structure. You now install and configure CA GovernanceMinder Discovery and Audit tools to work with Oracle RAC databases.

Integrate CA GovernanceMinder Discovery and Audit with Oracle RAC Databases

You integrate the CA GovernanceMinder Discovery and Audit tool with Oracle RAC databases to import and modify data, analyze, construct and administer the role hierarchy.

Follow these steps:

1. Run the CA GovernanceMinder Client Tools installer and open the application.

   The CA GovernanceMinder Client Tools installer, CA-RCM-*RN*-Client-Tools-x86.zip, is located in the folder where you downloaded the installation package files when you installed CA GovernanceMinder.

   Note: *RN* is the current release number for the product.

   The CA Role and Compliance Manager - Discover and Audit window appears.

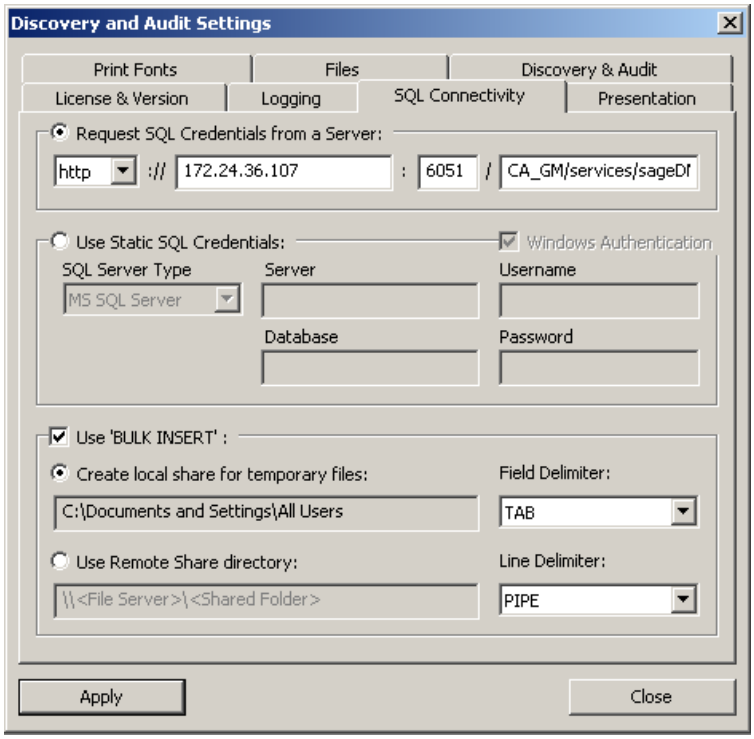
2. Navigate to File, General Settings.

   The Discovery and Audit Settings window appears.

3. In the SQL Connectivity tab, select Request SQL Credentials from a Server.

   This option connects the SQL database through the CA GovernanceMinder server.

   The following graphic displays the Request SQL Credentials from a Server option that is selected with an example server host IP address and port number displayed:



4. Enter in the CA GovernanceMinder server host name and the CA GovernanceMinder Server port number and click Apply.

   The Enter Server Credentials window appears.

5. In the SQL Server section, enter in the user name and password.

6. In the Web Server section, enter in the CA GovernanceMinder Portal administrator and password, and click OK.

7. In the Discovery and Audit Settings window, click Close.

   The CA GovernanceMinder Discovery and Audit tool is integrated to connect with Oracle RAC databases to manage data.

(Optional) Restore CA GovernanceMinder-Oracle RAC Databases Connection

You restore the connection between CA GovernanceMinder and Oracle RAC databases after a failure. Connection failures can occur when you connect to the SQL database through the CA GovernanceMinder server.

Follow these steps:

1. Edit the tnsnames.ora file for the database cluster from the database server. Do the following:
   a. Locate the tnsnames.ora file in the Oracle home directory.
   b. Locate the instances that represent your clustered service and verify your cluster address and port.

      Example:

      ```
      RCMDB1 =
         (DESCRIPTION =
           (ADDRESS = (PROTOCOL = TCP)(HOST = oraclusternode1-vip)(PORT = 1521))
           (ADDRESS = (PROTOCOL = TCP)(HOST = oraclusternode2-vip)(PORT = 1521))
           (LOAD_BALANCE = yes)
           (CONNECT_DATA =
            (SERVER = DEDICATED)
            (SERVICE_NAME = RCMDB1
         )
      )
      ```

   c. Save and close the file.

      The tnsnames.ora file is edited, and the Oracle client-server connection is restored.

2. Edit the eurekify.properties file to define the database host name as the CA GovernanceMinder SDB database. The SDB contains CA GovernanceMinder Master and Model data.

   Do the following:

   a. Locate the eurekify.properties file in the following folder:

      gm_install`/Program Files/CA\RCM/Server/eurekify-jboss/conf`

   b. Add the following property to define the database host name as the CA GovernanceMinder SDB database:

      `sdb.host=`*RCMDB1*

      Note: *RCMDB1* is the Oracle RAC database host name.

c. Save and close the file.

The eurekify.properties file is edited to define the database host name as the CA GovernanceMinder SDB database.

3. On the CA GovernanceMinder installation computer, open Oracle SQL Developer or similar program for working with SQL in Oracle databases.
4. Connect to the eurekify_sdb database, and insert the following text:

```
insert into SAGE_PREFERENCES
(LoginID, PrefGroup, Name, Value)
values
('eurekify.properties', 'eurekify.properties.dynamic', 'sdb.host', 'RCMDB1');
```

5. In the Query menu, select Execute to run the SQL query.

The CA GovernanceMinder and Oracle RAC databases connection is restored.

Using CA SiteMinder® to Support the Single Sign-On

This scenario describes how to use CA SiteMinder® to support the Single Sign-On (SSO) function for CA GovernanceMinder Portal users.

This scenario targets CA GovernanceMinder:

- System and database administrators
- System integrator

Chapter 7: How to Use 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.

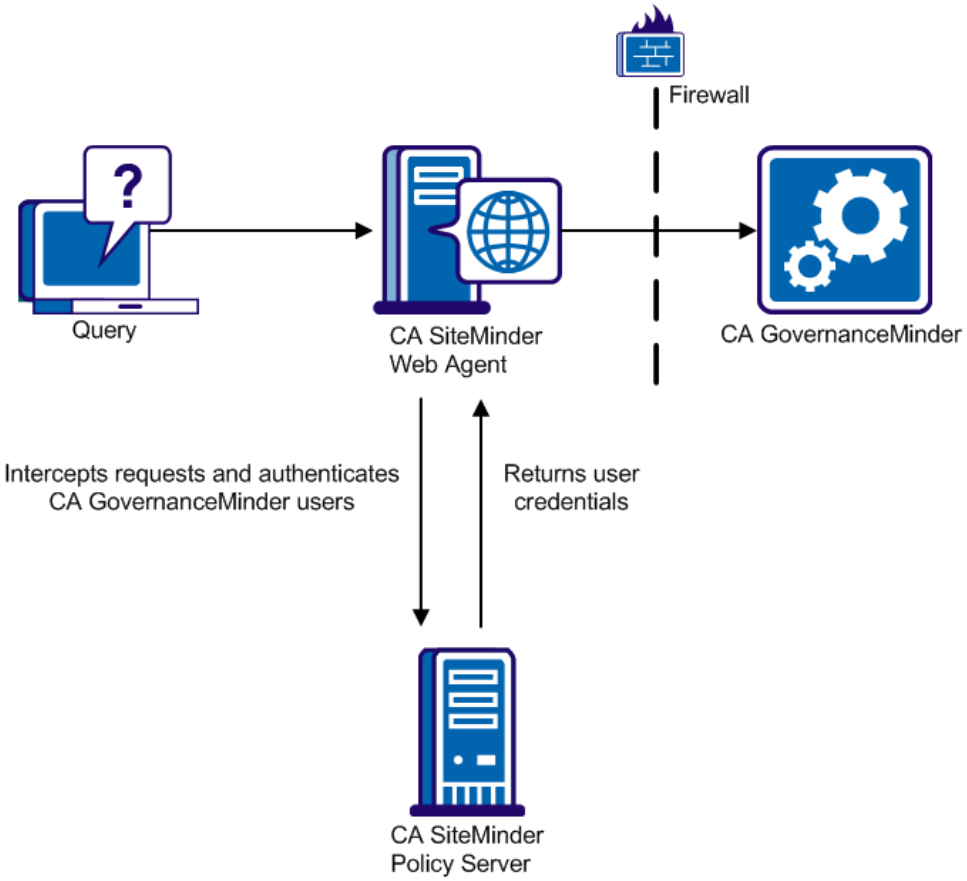
To implement SSO in the CA GovernanceMinder server environment, you must have the following CA SiteMinder® components:

- 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.

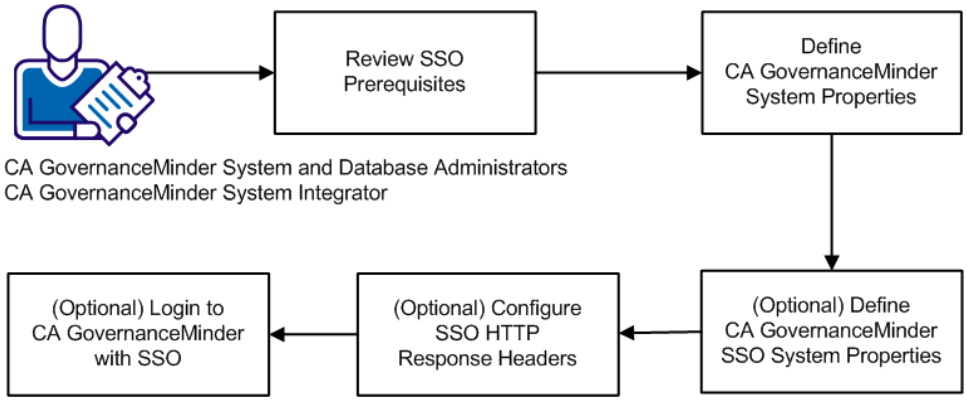
The CA GovernanceMinder and CA SiteMinder® servers are typically located behind enterprise firewalls, and the HTTP server with the CA SiteMinder® Web Agent is exposed to the public network.

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.
3. (Optional) Define CA GovernanceMinder SSO system properties.
4. (Optional) Configure SSO HTTP response headers.
5. (Optional) Login to CA GovernanceMinder with SSO.

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.

Chapter 8: Integrating CA User Activity Reporting with CA GovernanceMinder

This scenario describes how the system integrator integrates CA User Activity Reporting with CA GovernanceMinder.

Chapter 9: How to Integrate CA User Activity Reporting with CA GovernanceMinder

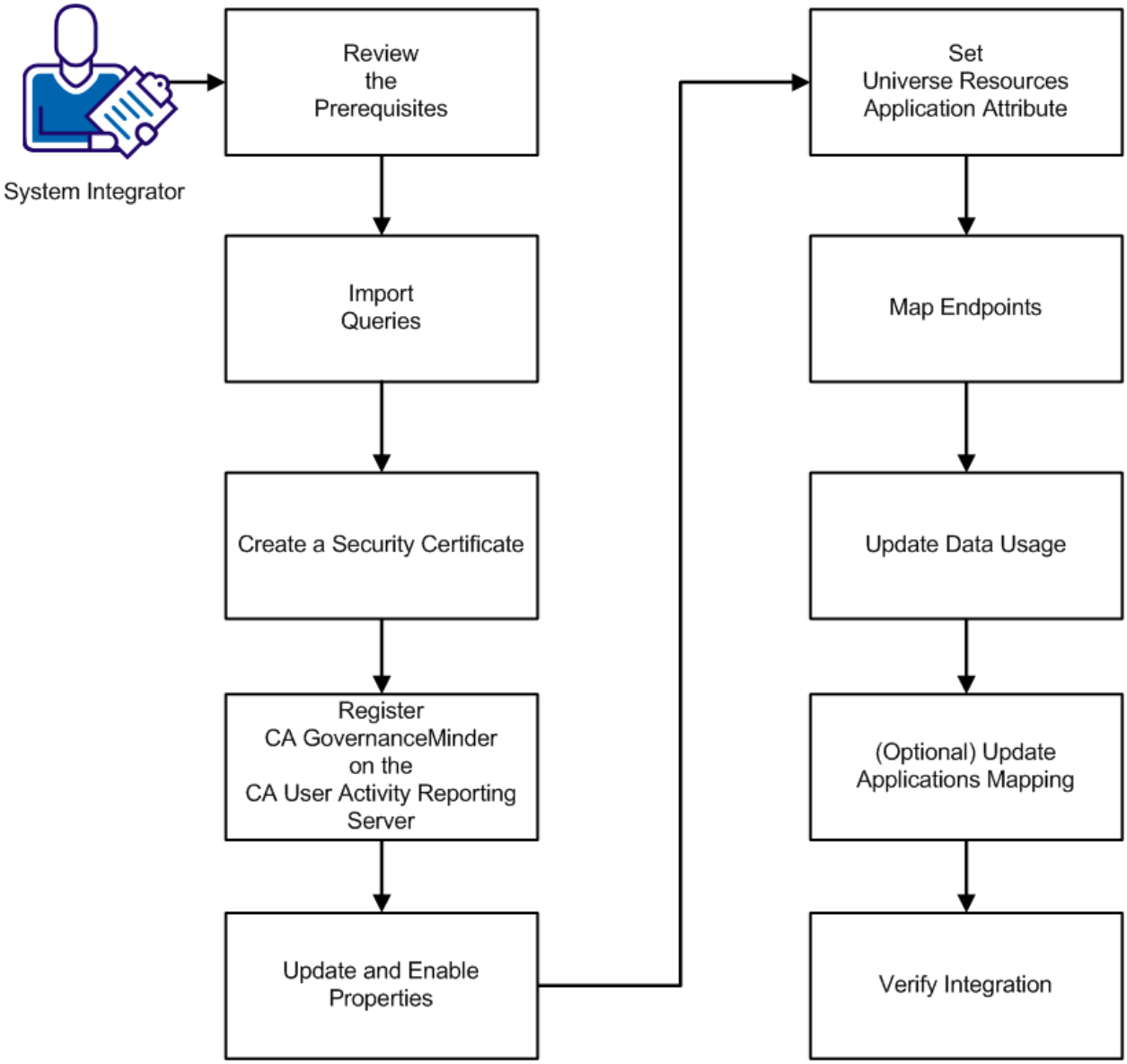
With CA User Activity Reporting integration, you can import CA User Activity Reporting data into CA GovernanceMinder, which then displays this data during certifications.

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 data to display during a certification.

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

Note: Enable CA GovernanceMinder integration with CA User Activity Reporting per universe.

The following diagram illustrates how to integrate CA User Activity Reporting:



To integrate CA User Activity Reporting, follow these steps:

1. Review the prerequisites (see page 77).
2. Import queries (see page 81).

3. Create a security certificate (see page 82).
4. Register CA GovernanceMinder on the CA User Activity Reporting server (see page 83).
5. Update and enable properties (see page 84).
6. Set universe resources application attribute (see page 85).
7. Map endpoints (see page 86).
8. Update data usage (see page 87).
9. (Optional) Update Applications Mapping (see page 88).
10. Verify integration (see page 88).

Review the Prerequisites

Before integrating the CA User Activity Reporting, perform the following actions:

Verify that you have a working CA GovernanceMinder universe with imported entities. If you are using CA Identity Manager in your environment, the system automatically imports account information. If you are not using CA Identity Manager, create an 'As Accounts' connector that maps to the endpoint that CA User Activity Reporting is monitoring, and use correlation rules (see page 78) to match the accounts to the user.

Note: Set the application attribute to ResName2 if you use the 'As Accounts' connector for the account information.

- To view events, install CA User Activity Reporting and create a user with permissions.
- 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 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.
- Correlate imported accounts to users (see page 78).
- (Optional) Import CSV data into an account configuration (see page 80).
- (Optional) Increase file handles (see page 81).

After you have reviewed the prerequisites, you import CA GovernanceMinder queries into CA User Activity Reporting.

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 Identity Manager, 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.

(Optional) 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. This special configuration 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.
5. Review CSV file structure.

   Review required fields for the CSV accounts data files. Each 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 comma-separated values.

Example: CSV accounts data file

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

```
personID,endpoint,account

5467238,UNXMARKT,jmeade

5467238,NT-Security,john_meade

7635097,RACFTEST,marcus432

6523876,NT-Security,kim_bell
```

You have manually imported account information from a CSV file into a special configuration that relates to the Model configuration of the universe and .reviewed CSV file structure.

(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 Queries

To import CA User Activity Reporting data into CA GovernanceMinder, add the CA GovernanceMinder data queries to the CA User Activity Reporting query list. CA GovernanceMinder calls these queries to display CA User Activity Reporting query results when users click monitored resources.

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.

Next, you create a security certificate.

Create a Security Certificate

To enable CA GovernanceMinder to communicate with CA User Activity Reporting, create a 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, open a browser to log in to the CA User Activity Reporting API portal and enter the following URL:
   `https://calm_hostname:port/spin/calmapi/calmapi.csp`

   A security certificate error appears.

   calm_hostname:port

   Specifies the CA User Activity Reporting server host name and communications port.
2. Click Continue to this website.

   A certificate error button appears to the right of the browser's address bar.
3. Click Certificate Error, View certificates.

   The Certificate dialog appears and displays information about the 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 server.

6. Update the keystore with the certificate, as follows:
   a. Open a command prompt and navigate to the directory that contains the exported certificate.
   b. 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.
   c. Enter the following password, or the default cacerts password for your system:

      'changeit'
   d. Enter y at the prompt and click Enter.

      The certificate is installed in the keystore.
7. Verify that the new certificate appears, as follows:
   a. At a command prompt on the server hosting computer, 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.

   You have created a security certificate and update the keystore with the new certificate.

   Next, you register CA GovernanceMinder on the CA User Activity Reporting server.

Register CA GovernanceMinder on the CA User Activity Reporting Server

To enable CA User Activity Reporting to recognize the certificate and enable connection to the CA GovernanceMinder server, register CA GovernanceMinder 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

   ELM_host

   Specifies the CA User Activity Reporting server host name.

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.

   CA GovernanceMinder is registered with the CA User Activity Reporting server.

   Next, you update CA GovernanceMinder properties.

Update and Enable Properties

To enable the CA GovernanceMinder server to communicate with CA User Activity Reporting and to enable CA User Activity Reporting online links, update and edit the CA GovernanceMinder system properties.

Follow these steps:

1. In the CA GovernanceMinder 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 host name 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 verify 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. 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 account that CA GovernanceMinder uses to log in.

   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.

usage.online.logmanager.eventviewer.enabled

Defines the CA User Activity Reporting online links. This property is disabled by default. Set to True.

Default: False

You have updated the system properties.

Next, you set the application attribute in the CA GovernanceMinder universe.

Set Universe Resources Application Attribute

To map applications between CA GovernanceMinder and CA User Activity Reporting, first specify which ResName (see page 85) attribute within the CA GovernanceMinder universe is associated with an application. **ResName2** is often a selected attribute, but this attribute depends on how you import data into the product. You must specify this attribute in the universe.

Follow these steps:

1. In the Portal, go to Administration, Universes, and select a universe to edit.
2. In the General tab, Configuration Resource Application Field, select the attribute that defines the application from the drop down menu.
3. Click Save.

   You have mapped applications between the product and CA User Activity Reporting.

   Next you map CA User Activity Reporting endpoints.

Resource Database File

Resource database file names end with the .rdb suffix. Each resource is represented in this file by one line, which includes comma-separated values for the following fields (in this order):

- Resource Name 1 (ResName1)
- Resource Name 2 (ResName1)

- Resource Name 3 (ResName1)
- (Optional) An unlimited number of additional fields

The ResName fields typically map to the endpoint or application group of the resource.

Although they are optional, CA GovernanceMinder requires you to specify fields for the following types of resource information when you define a universe. Define these fields in .rdb files that form the basis for a configuration file in a universe.

- Application
- ManagerID

Example: Resource Database File

The following sample file contains 3 resource records.

```
ResName1,ResName2,ResName3,Description,ManagerID-Owner,Location,
"SYS1","RACFPROD","RACF22","Production RACF","77292450","Irvine,CA",
"Domain Users","NT5AVE","WinNT","Active Directory ","91236370","Houson,TX",
"DEVELOP","RACFPROD","RACF22","Production RACF","77292450","Irvine,CA",
```

Map Endpoints

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 data is then correctly associated with CA GovernanceMinder resources.

Follow these steps:

1. In the Portal, go to Administration, Universes, and select a target universe.

   The Edit universe screen appears.

2. Under the Actual Usage tab, Settings, select Import and show usage data for this universe, and click Refresh Usage Data.

   Note: Import data from CA User Activity Reporting to obtain a list of all applications before mapping the applications to CA GovernanceMinder resources.

3. Click the Application Mapping tab.
4. In the Universe Applications section, select a CA GovernanceMinder application.
5. In the CA User Activity Reporting section, select the application that you want to map to the CA GovernanceMinder application.

6. Click Add.

   Mapped applications appear in the center pane.

7. Repeat these steps for all applications.

8. Click Finish to save settings.

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

   Next, you update data usage.

Update Data Usage

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

Follow these steps:

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

   The Universes 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 data usage, select Import and show data usage 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.

   Note: f 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, and then click Refresh Usage Details.

   You have updated usage data for the selected universe.

   Next you enable CA User Activity Reporting online links.

(Optional) Update Applications Mapping

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.

Follow these steps:

1. In the Portal, go to Administration, Universes, and select a target universe.

   The Edit universe screen appears.

2. Under the Actual Usage tab, Settings, select Import and show usage data for this universe, and click Refresh Usage Data.

   Note: Import data from CA User Activity Reporting to obtain a list of all applications before mapping the applications to CA GovernanceMinder resources.

3. Click the Application Mapping tab.

4. In the Universe Applications section, select a CA GovernanceMinder application.

5. In the CA User Activity Reporting section, select the application that you want to map to the CA GovernanceMinder application.

6. Click Add.

   Mapped applications appear in the center pane.

7. Repeat these steps for all applications.

8. Click Finish to save settings.

   You have updated CA User Activity Reporting applications mapping.

   Next, you verify the integration.

Verify Integration

When the integration is successful, you can view the user and resource information in the Entity Browser. This information is displayed in an information bubble that appears when you hover over a certification user with the mouse cursor.

In the Entity Browser, hover with the mouse pointer over a certificate user. An information bubble appears with the name of the resource, operating system, usage frequency, and the date last accessed.

Enable Certification

Product: CA GovernanceMinder

Release: 12.6.02

This scenario describes how a CA GovernanceMinder system administrator enables Active Directory, Lightweight Directory Access Protocol (LDAP), and Workpoint Server authentication.

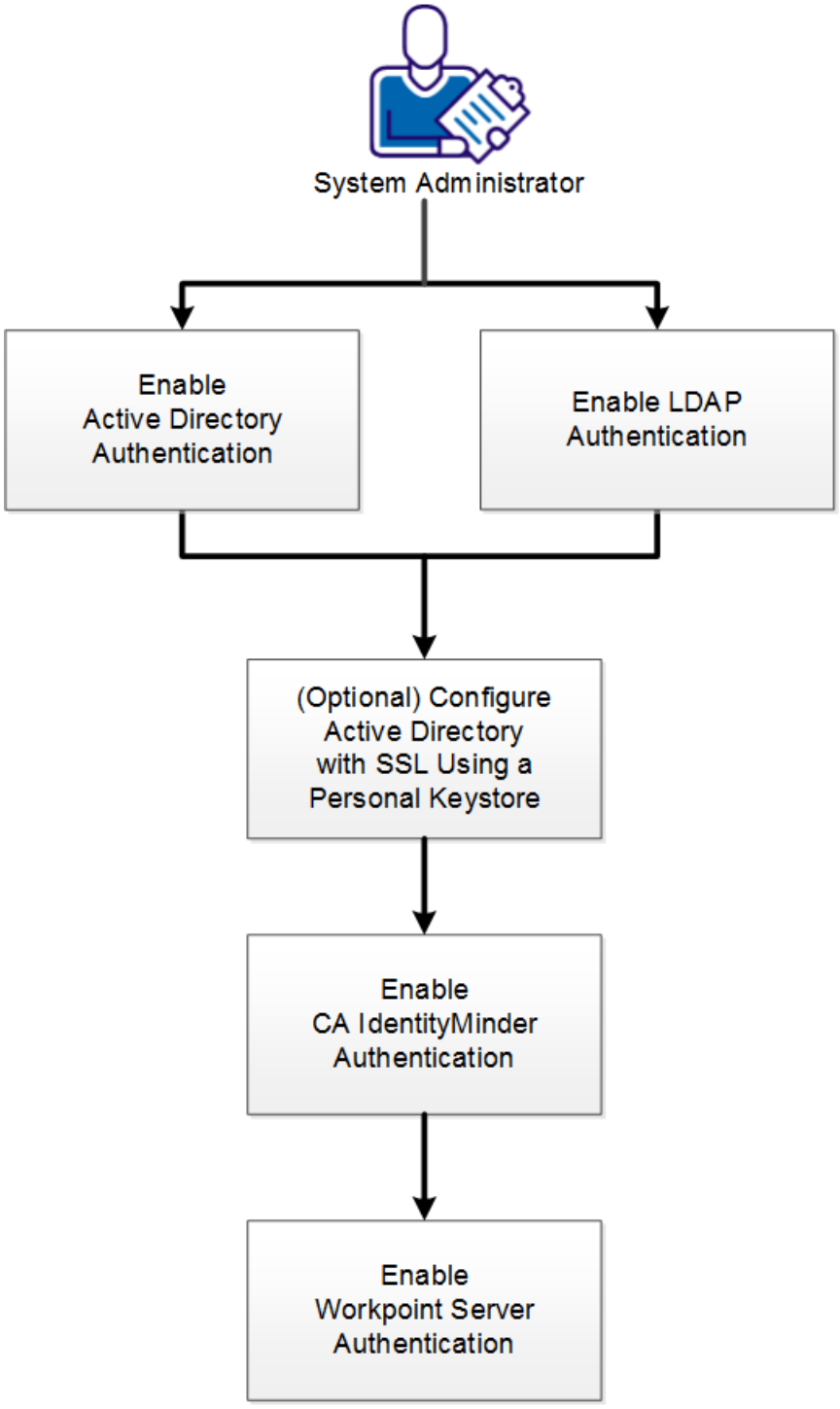
This Knowledge Base Article constitutes a portion of the official CA product documentation (<URL>) for this CA product. This Knowledge Base Article is subject to the following notices, terms, and conditions.

Enable Active Directory and Lightweight Directory Access Protocol (LDAP) Authentication

Authentication is the act of establishing that a user has sufficient security privileges to access the CA GovernanceMinder Portal. Active Directory is a service for Windows networks, and is included in most Windows Server operating systems. LDAP is the protocol for maintaining and accessing directory information over an IP network.

As a system administrator, you can authenticate user access to the CA GovernanceMinder Portal with Active Directory and LDAP.

The following diagram illustrates how to enable Active Directory, LDAP, and Workpoint server authentication:


System Administrator
Enable
Active Directory
Authentication
Enable LDAP
Authentication
(Optional) Configure
Active Directory
with SSL Using a
Personal Keystore
Enable
CA IdentityMinder
Authentication
Enable
Workpoint Server
Authentication

Follow these steps to configure CA GovernanceMinder for Active Directory and LDAP authentication:

1. Enable authentication for one of the following services or protocol:
   - Active Directory (see page 92)
   - LDAP (see page 95)
2. (Optional) Configure Active Directory with SSL using a personal keystore (see page 94).
3. Enable CA Identity Manager authentication (see page 96).
4. Enable Workpoint server authentication (see page 97).

Enable Active Directory Authentication

You enable Active Directory authentication by setting properties in the Portal.

Follow these steps:

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

   The Properties Settings window appears.

2. Set these property files as follows:

   sage.security.disable.ADAuthentication

   Defines the ability to enable Active Directory authentication. Set this value to False.

   Default: True

   security.ldap.server

   Defines the LDAP network server name or Active Directory IP address. (example: HOSTNAME.org.com)

   Default: adserver

   (Optional) security.manager.dn

   Specifies the distinguished name (DN) of the manager. The DN is often required only when using SSL authentication. The manager is *AD_bind_account* (example: administrator).

   Default: AD1\Administrator

   (Optional) security.manager.password

   Specifies the LDAP network administrator username. The Active Directory password is *AD_bind_account_password*.

   Default: eurekify

sage.security.credential.expiration.seconds

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

Default: 60

sage.security.eurekify.keyStore.file

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

Default: none

sage.security.eurekify.keystore.password

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

Default: none

Note: Use separate instructions if you want to use a personal keystore (see page 94) instead of the JVM keystore.

sage.security.disable.ssl.ADAUthentication

Defines whether you enable Active Directory authentication. Set this value to True to enable Active Directory authentication.

Defult: True

sage.default.domain

Defines the *Active_Directory_domain*.

Default: none

Note the following login issues:

- You must have a Login ID filed in the database with the domain name (example: *domain*\jsmith where *domain* is the domain name and jsmith is the login ID)
- 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, only the Login ID (jsmith).

(Optional) Configure Active Directory with SSL Using a Personal Keystore

You configure Active Directory with SSL using a personal keystore.

Follow these steps:

1. Download and install openSSL 1.0.1e from the Openssl website.
2. Open a command prompt and enter the following command:

   `openssl s_client -connect AD_server:636`

   Note: *AD_server* is the Active Directory server address.

   For example: openssl s_client -connect my_ad_server.ca.com:636.
3. Copy the 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

   Defines the keystore file path.

   Default: none

   sage.security.eurekify.keyStore.password

   Defines the server keystore password.

   Default: none

   Note: (Windows) Alternatively, you can also set Java Virtual Machine (JVM) properties (located 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 system LDAP server.

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

   Defines whether you enable Active Directory authentication. Set this value to False.

   Default: True

   security.ldap.server

   Defines the LDAP network server name.

   Default: adserver

   security.manager.dn

   Defines the distinguished name (DN) of the manager. The DN is often required only when using SSL authentication. The manager is *AD_bind_account* (example: administrator).

   Default: AD1\Administrator

   security.manager.password

   Defines the LDAP administrator password in your network.

   Default: eurekify

   security.authentication.ldap.server

   Defines the LDAP server host name.

   Default: none

   security.authentication.ldap.manager.dn

   Defines the LDAP administrator name.

   Default: none

   security.authentication.ldap.manager.password

   Defines the LDAP administrator password.

   Default: none

security.authentication.ldap.rootContext

Defines the name of the LDAP root context.

Note: Provide this value if the customer has a unique Active Directory layout, or to ensure that the user search views the sub tree level only.

Default: none

security.authentication.ldap.disable.ssl

Defines whether you enable SSL for CA Directory.

Default: none

security.authentication.ldap.lookupAttribute

Defines the LDAP attribute that uniquely identifies a user.

Note: This attribute corresponds to the PersonID attribute, which is a CA GovernanceMinder unique identifier.

Default: uid

security.authentication.ldap.disable

Defines if LDAP authentication is disabled. Set this value to False to disable LDAP authentication.

Default: True

You have enabled LDAP authentication.

Enable CA Identity Manager Authentication

When you enable CA Identity Manager authentication, the system authenticates users logging in to the Portal using CA Identity Manager. For more information about CA Identity Manager requirements, see the *CA Identity Manager Installation Guide*.

Follow these steps:

1. In the Portal, run an import from CA Identity Manager.

   Note: The authenticated user must exist in CA GovernanceMinder.

2. Under Administration, Settings, System Properties, set these properties as follows:

   sage.security.disable.IMAuthentication

   Defines whether you enablef CA Identity Manager authorization. Set this value to False to enable CA Identity Manager authorization.

   Default: True

   sage.security.IMAuthentication.universe

   Defines the universe name where you imported the users. See Step 1.

   Default: True

sage.default.IMdomain

Note: Due to legacy issues, this property must remain blank.

Default: none

(Optional) sage.security.disable.ADAuthentication

Defines whether you disable Active Directory authentication. Set this value to False.

Default: True

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

Note the following use cases around CA Identity Manager authentication:

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

Enable Workpoint Server Authentication

You can enable Workpoint server authentication.

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 these properties:

workpoint.connection.username

Defines the Workpoint user name.

workpoint.connection.password

Defines the Workpoint 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.