CA Identity Governance

CA Identity Manager Integration Guide

12.6.02a

CA Technologies Product References

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

Contact CA Technologies

Contact CA Support

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

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

Providing Feedback About Product Documentation

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

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

Contents

Chapter 1: Integration Overview

This section contains the following topics:

Integrating CA Identity Governance with CA Identity Manager

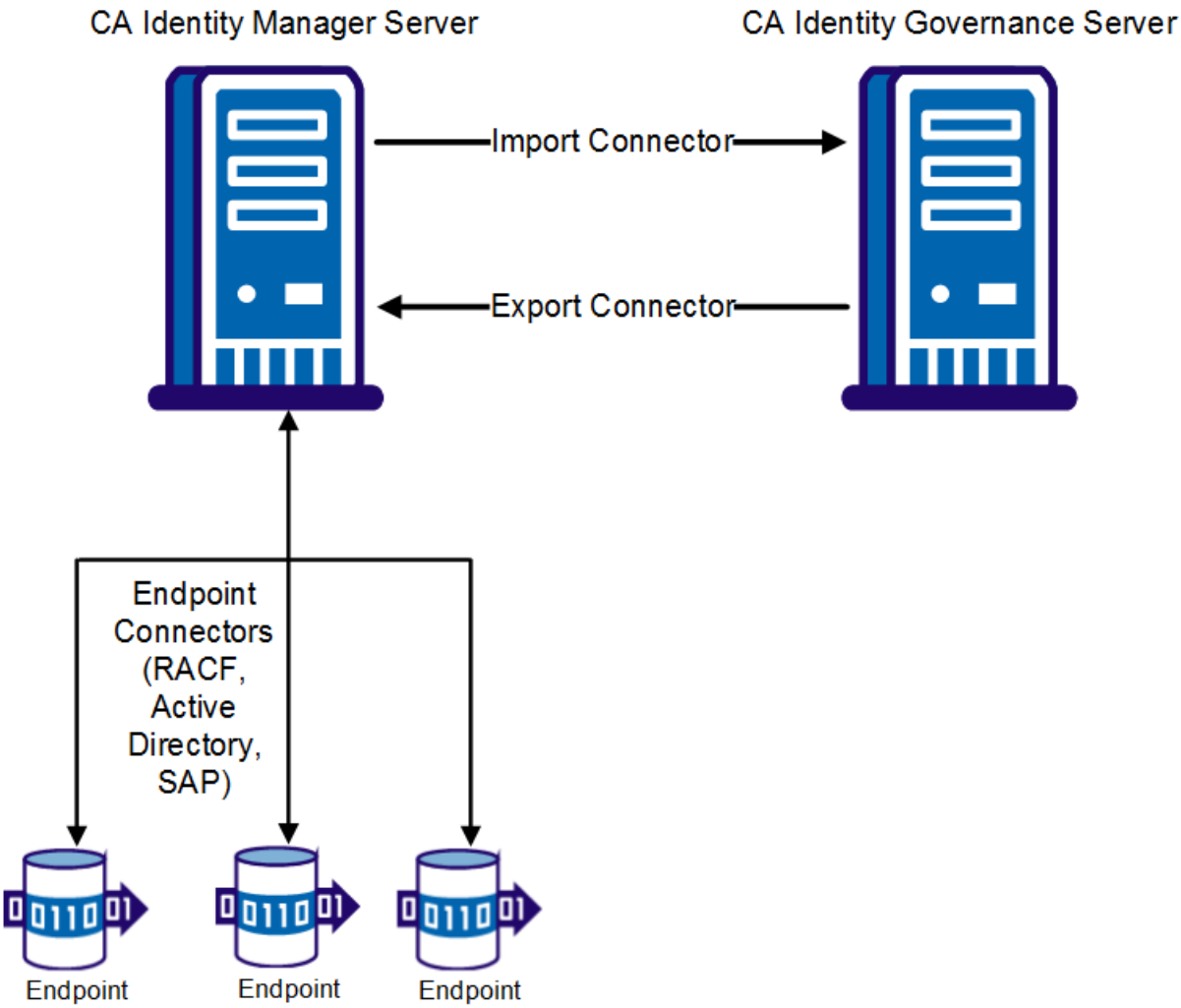
CA Identity Manager is an identity lifecycle management product that enables you to manage user identities and govern what they can access based on their role.

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

When you integrate CA Identity Manager and CA Identity Governance, you can do the following:

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

The following graphic details the architecture when you integrate CA Identity Governance and CA Identity Manager:



Use Case: Certifying CA Identity Manager Provisioning Role Assignments

As an Administrator, you want to allow managers to review and certify the provisioning roles of CA Identity Manager users they manage.

Perform the following process to allow managers to perform user certifications.

1. Integrate CA Identity Governance with CA Identity Manager.
2. Import data from CA Identity Manager to CA Identity Governance.

   This procedure updates the Master and the Model configuration in CA Identity Governance.
3. Kick off a user certification to review and approve user provisioning role assignments (and direct permissions).

   This certification updates the CA Identity Governance Model configuration.
4. Once the certification is completed, export the differences generated by the certification. The changes are applied to CA Identity Manager directly.

   CA Identity Manager records these changes in the task persistence database, where they can be viewed in the View Submitted Tasks task.

After completing this process, role assignment data between CA Identity Governance and CA Identity Manager is synchronized and approved by CA Identity Manager user managers.

Use Case: Maintaining Compliant CA Identity Manager Roles

As an Administrator, you want to be sure that when a new employee is added to CA Identity Manager, they automatically get privileges that are appropriate to their function within the company, and compliant with business policies.

Integrating with CA Identity Governance and enabling Smart Provisioning in an CA Identity Manager environment provides suggested roles and compliance checking when you create or modify users, roles, and accounts in CA Identity Manager.

For example, a new employee starts in the finance department at your company When you create the new user in CA Identity Manager, you specify that this person is part of the finance department. When you submit the Create User task in CA Identity Manager, CA Identity Governance returns a list of the following suggested roles for the new user:

- FinanceApplicationUser—This role allows access to the financial application.
- FinanceDept—This role gives general privileges to the new user that match other finance employees, such as an email account.

In addition, CA Identity Governance verifies that the existing privileges (if any) of the new user do not violate any business policy rules (BPRs).

Perform the following process to be sure that any new user added to CA Identity Manager gains the appropriate privileges that are compliant with company policy.

1. Integrate CA Identity Manager and CA Identity Governance.
2. Import CA Identity Manager user, role, and account data to CA Identity Governance.

   This procedure creates the Master and the Model configuration in CA Identity Governance.
3. Clean up the imported data in CA Identity Governance.

   This procedure removes suspect entities and suspect relationships between entities and updates the Model configuration.
4. Create Business Policy Rules (BPRs) in CA Identity Governance that reflect business restrictions and limitations regarding user privileges.
5. Run the BPRs created in Step 4 against the Model configuration.
6. Export any changes made to the Model configuration during Step 5 back to CA Identity Manager.

   This step updates the Master also.

After completing this process, CA Identity Governance suggests roles and performs compliance checks against business policy restrictions and limitations when you create and modify users, roles, or accounts in CA Identity Manager. Any day-to-day changes made in CA Identity Manager that affect users, roles, or accounts are updated in CA Identity Governance using Continuous Update.

Chapter 2: Integration Concepts

This section contains the following topics:

Import and Export

To introduce CA Identity Manager data to CA Identity Governance, you perform an import. The import process updates both the master and model configurations as follows:

1. The product creates a local copy of all the CA Identity Manager data.
2. The product compares the local copy with the master configuration. This results in a list of all changes since the last time the import ran.
3. The master configuration is updated with all the changes, and the master configuration now reflects everything in CA Identity Manager.
4. All changes are made in the model configuration, one by one. If the model configuration was the same as the master configuration, it will also be the same after the import. However, if there were changes made in the model, they are not overwritten by the import.

A CA Identity Governance universe is coupled with a CA Identity Manager Environment, and you import corporate users as the CA Identity Governance users. CA Identity Manager endpoint objects are imported as CA Identity Governance resources.

Important! Only one universe can be associated with a CA Identity Manager environment. If you must manage a different CA Identity Manager environment, create a new universe. If you delete a universe and create a new one, you must do a fresh import for the integration to work with the new universe.

You can customize the following data that you want to import:

- What types of endpoint objects to import. If you only want a subset of a particular object type, you can also apply filters to the data that is imported.
- What attributes are mapped to what CA Identity Governance fields.

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

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

- CA Identity Manager task model
- CA Identity Manager transaction logging
- CA Identity Manager policy triggers

Information Mapping between CA Identity Manager and CA Identity Governance

When CA Identity Manager and CA Identity Governance integrate, the following information is synchronized between the two systems:

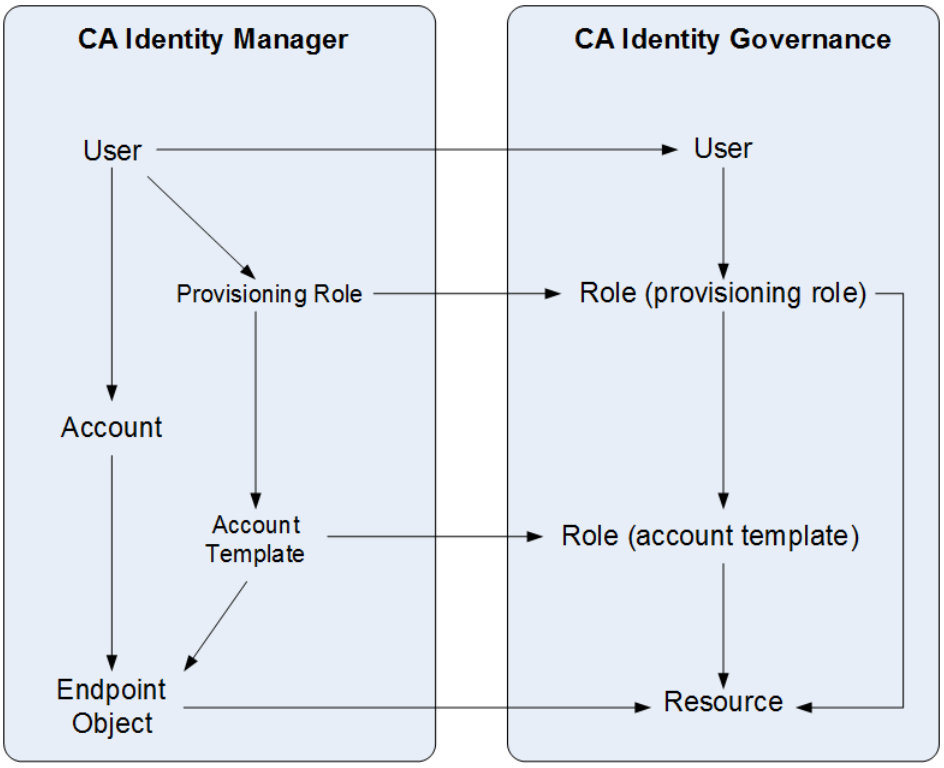
- User information
- Role information
- Account information
- Endpoint object information

The following table describes how information in one system maps to information in the other system.

CA Identity Governance Object	CA Identity Manager Object
User	User
Role	Provisioning Role or Account Template
Resource	Endpoint object that represents a privilege or role a user can have, for example: ■ Active Directory group ■ SAP profile ■ Oracle table privilege
User-Role link	User membership in a provisioning role
Role-Role link	Provisioning Roles or Account Templates

CA Identity Governance Object	CA Identity Manager Object
Role-Resource link	The relationship between a role and an account template that grants privileges on a specific endpoint.
User-Resource link	The relationship between a user and an endpoint object defined by an account.

The following graphic illustrates the information mapping between the two systems visually:



Communication between CA Identity Governance and CA Identity Manager

Once you configure integration between CA Identity Manager and CA Identity Governance, the two systems communicate using the following:

- CA Identity Governance Connector for CA Identity Manager (see page 32)

  A special type of connector that automatically synchronizes the privilege data between CA Identity Manager and CA Identity Governance. By using this connector, you can import data from CA Identity Manager to CA Identity Governance or export data from CA Identity Governance to CA Identity Manager.

  Note: For more information about connectors, see the *CA Identity Governance Configuration Guide*.

- Continuous Update (see page 24)

  This feature allows you to leverage CA Identity Governance capabilities to support day-to-day identity management operations. Any changes made in CA Identity Manager are updated immediately in CA Identity Governance.

- (Optional) Continuous Export (see page 46)

  This feature allows you to send any changes made in CA Identity Governance to CA Identity Manager immediately, instead of doing a full export operation after numerous changes are made to a role model.

Note: All of these communication features update the CA Identity Governance Master configuration.

Import Data from Multiple Endpoints

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

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

Importing information into a CA Identity Governance universe from any mix of two or more types of endpoints is referred to as mixed mode. A mixed universe can only support the shallow use case.

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

Connectivity Use Cases

Consider the following connectivity use cases when integrating with CA Identity Manager:

CA Identity Manager Managed Endpoints (see page 17)

Mixed Universe (see page 18)

Mixed Universe with Custom Endpoints - Example 1 (see page 19)

Mixed Universe with Custom Endpoints - Example 2 (see page 21)

Mixed Universe with Role Modeling (see page 22)

CA Identity Manager Managed Endpoints

Goal

You have an existing CA Identity Manager 12.5 SP8 (or later) deployment with a significant number of endpoints managed through the IAM Connector Server. You want to implement CA Identity Governance to perform certification on the privileges across the organization and use your existing IAM Connector Server connectors.

Environment Description

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

Process

1. Install CA Identity Governance, *without* including the IAM Connector Server.
2. In an CA Identity Governance universe, define a connector to CA Identity Manager, as follows:
   a. Define CA Identity Manager connectivity.
   b. Select all endpoints or use the 'all' wildcard.

3. Run an import.

   All endpoint data is imported into CA Identity Governance. The selected endpoint permissions are modeled as resources, while provisioning roles and account templates are modeled as roles.

Note the following:

- Export to the endpoints is fully supported in this scenario.
- CA Identity Governance correlation is not used, as CA Identity Manager provides the associations between users and accounts.

Mixed Universe

Goal

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

Environment Description

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

Process

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

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

3. In the universe, under the Connectivity tab, define a connector to CA Identity Manager. Within it, select the managed UNIX and Oracle endpoints. Select the CA Identity Manager Connector as the primary (As Users) connector.

4. Define connectors for the unmanaged endpoints (the ones you created in Step 2) by selecting the CA IAM Connector Server and, in each connector, select the correct endpoint.
5. Run a multi-import job by selecting all the connectors.

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

Note the following:

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

Mixed Universe with Custom Endpoints - Example 1

Goal

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

Environment Description

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

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

Process

1. Install CA Identity Governance.
2. After the new dynamic connector is ready, use Connector Xpress to push its definition to the CA IAM Connector Server installed with CA Identity Governance.
3. In the CA Identity Governance Portal, go to Administration, Connector Server Management.
4. Define the Active Directory server and the unmanaged UNIX and Oracle endpoints in the CA IAM Connector Server.
5. In the universe, go to the Connectivity tab.
6. Define a connector to CA Identity Manager. Select the managed UNIX and Oracle endpoints and set this connector as the primary (As Users) connector.
7. Define connectors for the unmanaged endpoints, including the dynamic connector, by choosing the CA IAM Connector Server and, in each connector, choosing the correct endpoint.
8. Run all the import connectors at once through a multi-import job.

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

Note the following:

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

Mixed Universe with Custom Endpoints - Example 2

Goal

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

Environment Description

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

Process

1. Install CA Identity Governance.
2. In the CA Identity Governance Portal, go to Administration, Connector Server Management.
3. Define the Active Directory server and the unmanaged UNIX and Oracle endpoints in the CA IAM Connector Server.
4. In the universe, go to the Connectivity tab.
5. Define a connector to CA Identity Manager. Select the managed UNIX and Oracle endpoints and set this connector as the primary (As Users) connector.
6. Define connectors for the unmanaged endpoints, including the dynamic connector, by choosing the CA IAM Connector Server and, in each connector, choosing the correct endpoint.

7. Define two connectors for the custom systems by selecting the PDI connector. Fill in the appropriate parameters for this connector.
8. Run all the import connectors at once through a multi-import job.

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

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

Note the following:

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

Mixed Universe with Role Modeling

Goal

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

Environment Description

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

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

Process

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

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

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

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

Note the following:

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

Workflow Approvals with Integration

When integrating with CA Identity Governance, CA Identity Manager workflow approvals are disabled for all export tasks generated by CA Identity Governance. All approvals for exported changes to CA Identity Manager must be handled in CA Identity Governance.

For example, if you run a User Certification, approvals are done as part of the certification. When you export all the changes to those users back to CA Identity Manager, no workflow processes are initiated for the CA Identity Manager tasks generated by that export.

Workflow behavior is unchanged for native CA Identity Manager tasks within the system.

If you have workflow processes in CA Identity Manager that you want to enforce when doing approvals in CA Identity Governance, you must recreate those workflow processes in CA Identity Governance.

Note: CA Identity Manager tasks generated by an CA Identity Governance export contain 'IMRCM' in the task name.

Continuous Update

To support integration, certain changes made in CA Identity Manager are queued up and passed to CA Identity Governance. This feature allows CA Identity Governance to make provisioning role suggestions and validate changes against compliance policies, based on current CA Identity Manager information, instead of waiting for another import from CA Identity Manager to update the CA Identity Governance data.

When a user, role, or account change occurs, CA Identity Manager generates a notification and adds it to a queue. At specified intervals, CA Identity Manager creates an aggregate notification with all the information in the queue (up to the maximum batch size) and sends it to CA Identity Governance.

CA Identity Manager continuously updates CA Identity Governance when the following events occur:

- Creating, modifying, or deleting a user
- Creating, modifying, or deleting provisioning roles
- Adding an account template to a provisioning role
- Creating, modifying, or deleting an account
- Creating, modifying, or deleting an account template
- Assigning an account to a resource or removing an account from a resource

- Assigning an account template to a resource or removing an account template from a resource
- Adding a provisioning role to a provisioning role (nested roles) or removing a provisioning role from a provisioning role

Continuous updates occur automatically when an active connection to CA Identity Governance exists in an CA Identity Manager Environment.

Continuous Update Exception Handling

If issues occur between CA Identity Manager and CA Identity Governance while they are integrated, CA Identity Manager processes the notification queue accordingly so that the queue does not become too large. The following table lists the possible exceptions and how CA Identity Manager handles the notification queue in each scenario.

Exception Source	CA Identity Manager Action
Network issues such as the following: ■ network down ■ server down ■ invalid port ■ invalid credentials	CA Identity Manager returns all notifications back to the queue. CA Identity Manager tests the connection to CA Identity Governance during the next cycle and resends the batch if the network connection is back up.
CA Identity Governance universe deleted	CA Identity Manager deletes the CA Identity Governance connection object for the environment and stop queuing notifications.
CA Identity Manager environment deleted	CA Identity Manager flushes the queue of all notifications for the environment.
CA Identity Governance can not queue notifications, for example, if the JMS queue is down.	CA Identity Manager retries to send the batch of notifications on the next cycle, as many times as the specified retry limit. When CA Identity Manager reaches the retry limit, the entire batch of notifications are deleted from the queue.
CA Identity Governance internal server exception, for example, out of memory.	CA Identity Manager returns all notifications back to the queue. During the next cycle, CA Identity Manager retries to send the batch. If an exception occurs again, CA Identity Manager removes the entire batch from the queue.

Chapter 3: Integrating with CA Identity Manager

This section contains the following topics:

Prerequisites for CA Identity Governance Integration

To integrate CA Identity Manager and CA Identity Governance, verify that the following prerequisites are met:

- CA Identity Governance and CA Identity Manager must be installed on systems that can communicate with each other

  Note: For more information, see the *CA Identity Governance Installation Guide* and the *CA Identity Manager Installation Guide.*

- If you want to secure the connection between CA Identity Manager and CA Identity Governance, configure both systems to support SSL.

- Be sure that you have imported all role definitions files for every endpoint type you have in CA Identity Manager.

- Be sure that all provisioning roles are managed by CA Identity Manager (and *not* the Provisioning Manager).
- If you are using Microsoft SQL as the Identity Manager user store, do the following:
  1. (JBoss only) In CA Identity Governance, download the sqljdbc.jar from the Microsoft Download Center and put it in the following location:

     `JBoss:`
     `RCM_Server_home\eurekify-jboss\server\eurekify\deploy\eurekify.war\web-inf\lib`
  2. In CA Identity Manager, go to the Management Console and do the following:
     a. Go to Environments and click the Identity Manager Environment you want to integrate with.
     b. Click Advanced Settings, Miscellaneous.
     c. Enter the property name "rdbdirpassword" with a valid user store password as the value.
     d. Click Add.
     e. Click Save.

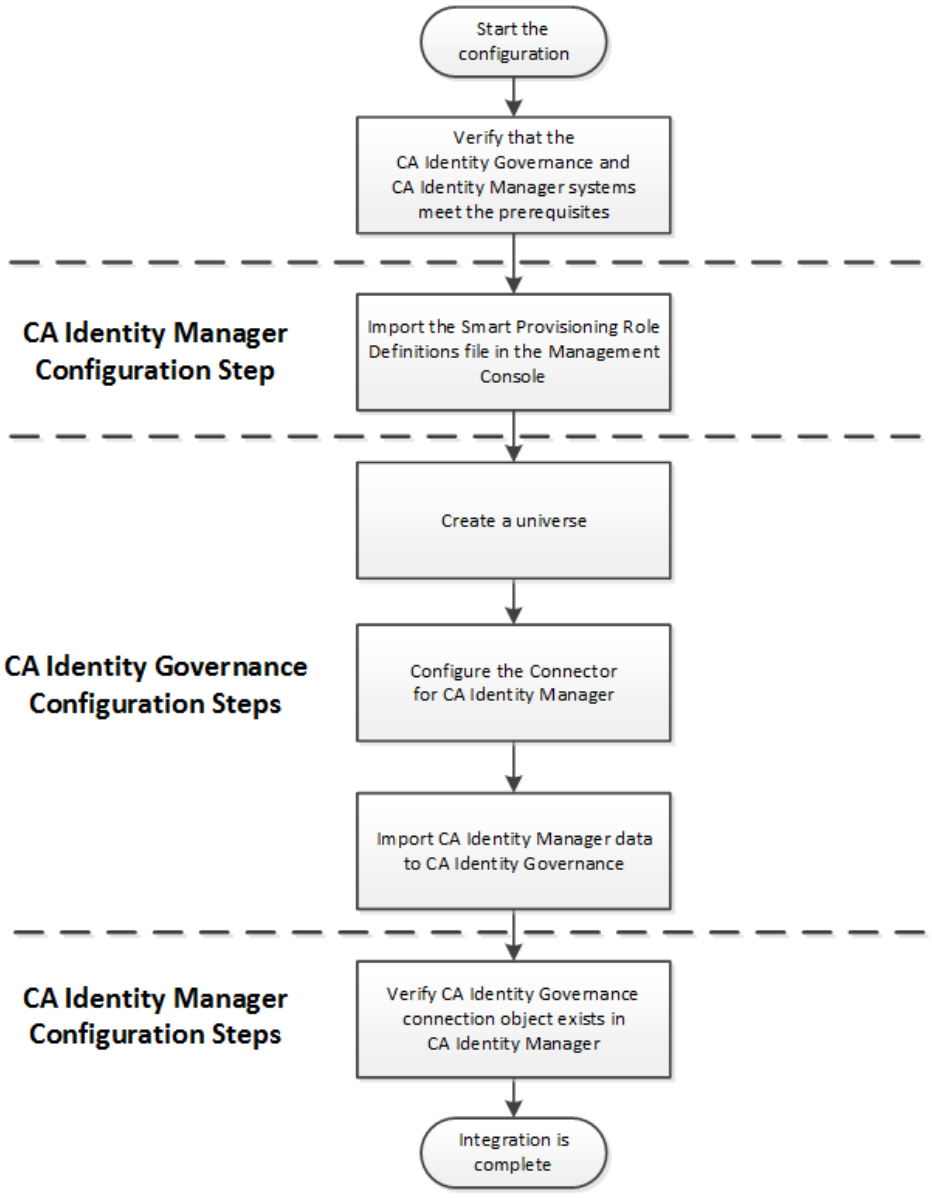
How to Configure Integration

Perform the following steps when you configure integration with CA Identity Governance.

1. Verify that the systems that host CA Identity Governance and CA Identity Manager meet the prerequisites (see page 27).
2. In CA Identity Manager, add integration support to your environment by importing the Smart Provisioning role definitions.

   Note: The Smart Provisioning role definitions include the tasks that you use to configure the connection to CA Identity Governance in the User Console.
3. In CA Identity Governance, complete the following steps:
   a. Create a universe.
   b. Configure an import connector to CA Identity Manager.
   c. Import data from CA Identity Manager to CA Identity Governance. This import creates a CA Identity Governance role model.
4. Verify that a CA Identity Governance connection object was created in CA Identity Manager.

The following flowchart illustrates the steps required to configure integration between CA Identity Manager and CA Identity Governance.



Import Role and Task Definitions for Integration

To configure CA Identity Manager to work with CA Identity Governance, you add a set of role and task definitions to a CA Identity Manager environment.

To import role and task definitions

1. In the Management Console, click Environments.

   A list of CA Identity Manager environments appears.

   Important! If this environment was created in a previous release of CA Identity Manager, be sure that you updated the role definitions after the upgrade and before performing the following steps. For more information about updating role definitions for an environment, see the *CA Identity Manager Upgrade Guide* for your application server.

2. Click the name of the CA Identity Manager environment where you want to import the role and task settings.

   The Properties screen for that environment appears.

3. Click Role and Task Settings, and click Import.

4. Select the Smart Provisioning role definitions file to create default roles and tasks for the environment.

   Note: The Smart Provisioning role definition file includes tasks that you use to configure the connection to CA Identity Governance in the User Console. Import this file even if you do not plan to use the Smart Provisioning functionality.

5. Click Finish.

   The status is displayed in the Role Configuration Output window.

6. Click Continue to exit.

7. If the CA Identity Manager environment was running, restart the CA Identity Manager environment.

Create a Universe in CA Identity Governance

Similar to an CA Identity Manager environment, a universe is a view into a management workspace that lets CA Identity Governance administrators manage entities such as users, roles, and resources collected from CA Identity Manager. Entity data is stored in the CA Identity Governance database. A universe consists of a specific pair of Master-Model configurations, enabling tracking of differences between the real-world configuration imported from the system (Master) and the desired configuration generated (Model).

To import data from CA Identity Manager, you need a universe in CA Identity Governance to store the data.

You need the following information to create a universe within CA Identity Governance:

- Master configuration file name
- Model configuration file name

  Important! You must provide names of configuration files that do not exist yet. Example configuration file names: CA_IMmaster.cfg, CA_IMmodel.cfg.
- (Optional) Approved Audit Card
- Names of the fields (in the configuration files) that contain the following information:
  - Login
  - Email
  - User manager
  - Role manager
  - Resource manager
- Audit Settings file name

Note: For more information about creating a universe, see the *CA Identity Governance Configuration Guide*.

How to Define an Import Connector to CA Identity Manager

CA Identity Governance imports data from CA Identity Manager by using an import connector. To define the connector, perform the following procedures.

1. Define the connection parameters to access CA Identity Manager.
2. Define the data mappings to define how the connector maps CA Identity Manager objects to CA Identity Governance objects.

Once you define the import connector to CA Identity Manager and run an initial import, CA Identity Governance automatically creates a CA Identity Manager connection object back to CA Identity Governance.

To define an import connector

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

   A list of universes appears.
3. Click on the universe you want to import data to.
4. Select the Connectivity Tab.

   The Connector screen opens.

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

   The Connector wizard appears.

6. Provide values for all mandatory connector settings and mappings.

7. Click Finish

   The new import connector is defined in CA Identity Governance.

8. (Optional) Click the Owner link next to the new connector and set a user as the owner of the connector. This user is notified by email if the connector fails during an import or export job.

9. (Optional) Select the new connector and click Validate.

   The connector parameters and configuration are validated.

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

Define a Connector to CA Identity Manager

To define an import connector to CA Identity Manager, use the import connector wizard under the connectivity tab of the universe. The wizard guides you through mapping Identity Manager users, roles, and account templates to CA Identity Governance.

The following steps are reflected in the connector wizard. Perform these steps to define a connector to CA Identity Manager.

1. (Connection Settings) Configure the connectivity between CA Identity Manager and CA Identity Governance. Provide the following connection information:

   - Identity Manager Server information and Identity Manager environment credentials.

     Be sure to use the login name of a CA Identity Manager administrator who has admin roles with the following tasks:

     - Create Web Services Configuration
     - View Web Services Configuration
     - Modify Web Services Configuration
     - Delete Web Services Configuration

- DefineCARCMConnection - included in the CA Identity Governance Configuration Manager role.
- DeleteCARCMConnection - included in the CA Identity Governance Configuration Manager role.

Note: For instructions on adding admin tasks to an admin role, see the topic Select Admin Tasks for the Role in the Admin Roles chapter in the *CA Identity Manager Administration Guide*.

If you have SiteMinder in your deployment, set the CA Identity Manager port to 80.

- CA Identity Governance Server information and credentials

  Note: The Register RCM Connection check box is selected by default. This option causes the import to automatically create the CA Identity Governance connection object within CA Identity Manager. Clearing this check box supports the use case of importing one Identity Manager environment into several CA Identity Governance universes. Because Continuous Updates and Smart Provisioning can only work with one universe, if you configure multiple universes to one Identity Manager environment, each time you run an import, it changes the CA Identity Governance connection object in CA Identity Manager to point to the universe you are importing to. By clearing this check box, the import process does not try to create or change the CA Identity Governance connection object within CA Identity Manager.

- The CA Identity Governance universe to be associated with the Identity Manager environment.
- The Additional Connection Properties area is only used for setting the FIPSKeyFile property.

2. (Identity Manager Users and Provisioning Roles) Map Identity Manager users to CA Identity Governance users and provisioning roles to CA Identity Governance roles.

   Note the following:

   - Click Add in the right-hand corner of the User Mapping section to add more user mappings between CA Identity Governance and CA Identity Manager.
   - Mapping fields are case-sensitive.
   - Use the filter to import a subset of users or provisioning roles from CA Identity Manager.
   - CA Identity Manager users and provisioning roles are automatically populated in the drop-down list.
   - You can enrich imported user data with supplementary Human Resources (HR) data.

3. (Endpoint Types) Define mappings (see page 34) between endpoint objects and CA Identity Governance resources.

   Note the following:

   - Be sure that you have imported all role definitions files in CA Identity Manager for every endpoint type that you have, otherwise they do not appear in the endpoint type drop-down list.
   - Mapping fields are case-sensitive.
   - For more information about endpoints, and endpoint objects and attributes, see the Endpoint Guides on CA Support.
   - You can enrich imported endpoint data with supplementary resource data.

4. (Summary) Review the connector information and click Finish to save the connector.

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

Define Endpoint Mappings

This section of the connector wizard allows you to map endpoint objects to CA Identity Governance objects.

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

To define endpoint mappings

1. Select the endpoint type from the drop-down list on the right and click Add.
2. Under Account Template, select account templates for following fields:

   Copy From

   Defines the existing account template in CA Identity Manager. This is used during an export. If an account template is created by CA Identity Governance, it only knows about some of the account template attributes. CA Identity Governance uses the existing account template to create a full attribute list when creating a new account template in CA Identity Manager during export.

   Create Account From

   Defines the account template used to create an account when a user does not have an account on the endpoint. This is used during an export.

3. (Optional) Use the Account Template filter to import a subset of account templates from CA Identity Manager.
4. Under Field Mapping, map account template attributes to CA Identity Governance role fields.

5. Under Endpoint List, click Add on the right to add an endpoint.
6. Under Endpoint Name, select an endpoint based on a pattern, or select an endpoint by name.
7. Under Endpoint Template, select one of the following:
   - (Recommended) Use template—loads a default template for the endpoint, mapping endpoint objects to appropriate CA Identity Governance resources.
   - Use template from file—allows you to browse and load an existing endpoint template from a file.

Note: If you want to adjust the endpoint mappings of a loaded template, select the Customize Selected Endpoint Template check box.

- Use custom configuration (see page 35)—allows you to create your endpoint configuration manually.

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

1. Click Next.
2. Repeat Steps 5 through 8 for each endpoint.
3. Click Ok.
4. Return to Step 1 and repeat the entire process per endpoint type.

Define a Custom Configuration for the Endpoint

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

If you select Use custom configuration for your endpoint template, you must manually provide mappings between CA Identity Manager and CA Identity Governance so that both systems understand the relationships between objects.

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

   Note the following:

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

2. Click Next.

3. Define associations (see page 37) for the endpoint. This screen allows you to do the following:

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

   Define associations as follows:

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

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

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

   d. Click Ok.

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

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

      Click Ok.

4. At this point, the object that the account is associated to does not yet relate to a known CA Identity Governance resource. Define the relation to a resource as follows:

   a. Click the 'Select RCM role/resource' active link.

   b. Provide a name for the CA Identity Governance resource.

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

      You can map attributes on the endpoint object to fields on the CA Identity Governance resource.

   d. Click Ok.

5. Repeat Steps 3 and 4 for each association.

6. Click Ok.

Associations Overview

Object in CA Identity Manager compared to objects in CA Identity Governance

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

The Issue

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

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

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

Example

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

Working with Associations

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

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

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

Custom Association Attributes (Link Attributes)

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

Enrichment

During an import, you can merge supplementary Human Resources (HR) data or additional role and resource data with the existing users, roles, and resources databases.

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

A supplementary enrichment file must be in CSV file format.

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

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

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

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

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

Clear Fields that are empty in the enrichment file

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

Hide the Custom Configuration Option in the Connector Wizard

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

universe.property.*universe_name*.endpointAssociations.enabled

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

Default: True

Map Person ID to Ensure Unique User IDs

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

- smijo09 - John Smith
- jsmith - John Smith

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

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

Import CA Identity Manager Data to CA Identity Governance

After you define the connector between CA Identity Manager and CA Identity Governance, you can import information about users, roles, and endpoint privileges into CA Identity Governance. Role engineers can then analyze that data using various tools in CA Identity Governance. Once the role engineers determine the role structure, they can apply changes, based on that structure, to CA Identity Manager.

You import data from endpoints managed by CA Identity Manager by defining connector jobs in the CA Identity Governance portal. You can then run a connector job, or define a schedule that automatically runs a job at specified intervals.

Note: For more information about running an import connector job, see the *CA Identity Governance Configuration Guide*.

The import creates the configuration files (CFG) you specified in the universe and populates them with CA Identity Manager data. Also after import, the connection object between CA Identity Manager and CA Identity Governance is automatically created.

Verify the Connection to CA Identity Manager

A connection to CA Identity Governance is automatically configured in CA Identity Manager to enable integration. Verify that the connection object in CA Identity Manager was created.

To verify the connection object to CA Identity Governance

1. Log in to the User Console as a user with system management privileges.
2. Go to System, CA Identity Governance Configuration, Define Configuration.

   The CA Identity Governance connection details are automatically populated under the Connection Settings tab.

   This connection object also defines the Smart Provisioning and Continuous Update settings that are also made available after the initial import.
3. Click Test Connection to verify that CA Identity Manager can connect to CA Identity Governance.

   CA Identity Manager displays the connection status at the top of the screen.
4. Click Cancel.

   CA Identity Manager can now successfully communicate with CA Identity Governance.

Note: If there is a problem with the connection object, manually configure a connection to CA Identity Governance (see page 41).

Manually Configure a Connection to CA Identity Governance

If a connection to CA Identity Governance was not automatically created within CA Identity Manager, configure a connection manually to CA Identity Governance. This allows you to see Smart Provisioning functionality and configuration options in the User Console.

To manually configure a connection to CA Identity Governance

1. Log in to the User Console as a user with system management privileges.
2. Go to System, CA Identity Governance Configuration, Define Configuration.

   Note: Do not use other connection tasks in the User Console to create the connection to CA Identity Governance.

   The Connection Setting tab appears.

3. Enter the following information about the system where CA Identity Governance is running:

   Host

   The fully qualified name or IP address of the system where CA Identity Governance is installed.

   Port

   The port number for CA Identity Governance.

   User ID

   The name for an account that has privileges to access CA Identity Governance.

   Password

   The password for the account specified in the User ID field.

   Secure Connection (HTTPS)

   Enables an HTTPS connection between CA Identity Manager and CA Identity Governance.

   Note: You must have SSL configured to secure the connection between CA Identity Manager and CA Identity Governance.

4. Enter the following information about CA Identity Governance:

   Universe

   The name of the universe in CA Identity Governance that CA Identity Manager communicates with.

   A universe is a virtual location in CA Identity Governance that encompasses the data collected from CA Identity Manager.

   Note: You create a universe in the CA Identity Governance Portal. For more information, see the *CA Identity Governance Configuration Guide.*

5. Click Test Connection to verify that CA Identity Manager can connect to CA Identity Governance.

   CA Identity Manager displays the connection status at the top of the screen.

6. Click Submit.

   CA Identity Manager can now successfully communicate with CA Identity Governance.

Edit Continuous Update Settings

When integrated, CA Identity Manager notifies CA Identity Governance of changes at frequent intervals. Continuous updates provide CA Identity Governance with the most current CA Identity Manager information.

When a user, role, or account change occurs, CA Identity Manager generates a notification and adds it to a queue. At specified intervals, CA Identity Manager creates an aggregate notification with all the information in the queue (up to the maximum batch size) and sends it to CA Identity Governance.

To edit continuous update settings

1. Log into the User Console as a user with administrative privileges.
2. Go to System, CA Identity Governance Configuration, Define Configuration.

   The Configuration Screen appears with the following tabs, Connection Settings, Smart Provisioning, and Continuous Update.
3. Under the Continuous Update tab, set the following defaults:

   Post Notifications to Queue

   Enables the queuing of notifications for all CA Identity Manager tasks that complete successfully. If you clear this check box, no notifications are queued to be sent to CA Identity Governance.

   Note: This check box can be selected even if the CA Identity Governance connection is disabled, meaning notifications are queued until the connection is re-established.

   Send Queued Notifications

   Enables the sending of notifications queued up in the analytics queue. If you clear this check box, CA Identity Manager suspends the sending of notifications to CA Identity Governance. If the CA Identity Governance connection is disabled, no notifications from the analytics queue are sent to CA Identity Governance. If the Queue Notification check box is cleared, this check box is cleared also. No notifications can be sent if you do not queue the notifications.

   Note: You may want to disable the sending of notifications if the CA Identity Governance Server is unavailable.

Maximum Notification Batch Size

Defines the maximum number of notifications that are read from the queue and sent to CA Identity Governance in a batch for that interval.

Default: 1000 notifications

Notification Batch Transmit Interval

Specifies the interval in seconds, minutes, or hours between times when CA Identity Manager sends a batch of notifications from the queue to CA Identity Governance.

Default: 59 seconds

Minimum: 1 second

4. Click Submit.

Chapter 4: Exporting Data to CA Identity Manager

This section contains the following topics:

Export to CA Identity Manager

Important! Enable the model fix (see page 46) before exporting to CA Identity Manager, otherwise the export detects model compatibility issues and exits.

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

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

- CA Identity Manager task model
- CA Identity Manager transaction logging
- CA Identity Manager policy triggers

Note: When you define a CA Identity Manager Connector in CA Identity Governance, a matching export connector is automatically defined.

If you are exporting many changes to CA Identity Manager, and the export takes a long time, you can use the following property to tune the export to CA Identity Manager:

connectors.im.export.thread.pool.size

Defines the thread pool size for an export to CA Identity Manager.

Default: 15

Continuous Export

For CA Identity Governance to continuously send data to CA Identity Manager, instead of waiting for the next export to send over bulk changes, enable continuous export. To enable continuous export, select the CONTINUOUS_EXPORT check box in the Connector (Export) screen. Also, in the CA Identity Governance Portal, go to Administration, Settings, Property Settings and set the following properties:

- modelEvent.producer.fireEvent: Set to a permitted value - AGGREGATE, or ATOMIC
- approval.isModelChangeNotificationOn: TRUE
- modelEvent.notify.topic: TRUE

CA Identity Manager Model Fix

Important! Enable the model fix before exporting to CA Identity Manager, otherwise the export detects model compatibility issues and exits.

While working in CA Identity Governance, you may change a Model configuration and create a scenario that is not supported in CA Identity Manager. For example, CA Identity Manager does not allow a resource to be linked directly to a provisioning role. The export process to CA Identity Manager can fix any issues with the Model configuration and ensures that every user maintains the same privileges it had before the fix.

The CA Identity Manager model fix corrects invalid links between roles to resources and users.

Note: Configurations imported using legacy connectors are fixed using the legacy autofix functionality.

In the Connectivity tab of the universe, in the export screen, you can select one of the following model fix options:

- Automatic—if errors are found in the model, corrections are made during export.
- Manual—if errors are found in the model, this option creates a business workflow and sends it to the administrator for approval.

Note: To analyze a universe and fix configurations with invalid links manually, go to Administration, Settings, Autofix IM Configuration.

- No—if there are errors, no corrections are made to the configuration and the export does not run.

The following building blocks were added and can be used in the export processes:

- AutoFixCheck—returns true/false(configuration has invalid links)
- AutoFixConfiguration—fix the configuration

Model Compatibility

When you integrate CA Identity Governance and CA Identity Manager, the following incompatibility can occur.

CA Identity Governance privileges are additive, meaning that a user is given every privilege dictated by the roles that they belong to. However, in CA Identity Manager, an account can be subtractive, meaning that a user can have fewer privileges than its account template dictates.

The normal import and export process between CA Identity Governance and CA Identity Manager does not detect the difference between assigned privileges due to the previous issue, so there is a discrepancy between CA Identity Manager data and CA Identity Governance data.

CA Identity Governance detects missing privileges during an import process, and then adds the missing privileges during export. To enable this solution, select the Model Compatibility check box under the Connectors (Export) screen.

Note: Model compatibility is not run during continuous export. To retain this functionality, schedule a full export to run at regular intervals.

Change the CA Identity Governance Export Administrator

To run tasks associated with the CA Identity Governance export in CA Identity Manager, an administrative user is selected to run the task. CA Identity Manager selects an administrative user that has the System Manager role. If you want to change the administrative user to run CA Identity Governance export tasks, go to System, CA Identity Governance Configuration, Change Export Administrator and select a new user.

The selected user will be a member of the role associated with the web services configuration of CA Identity Governance export. This user does not have to have a system manager role.

Chapter 5: Smart Provisioning

This section contains the following topics:

Smart Provisioning Overview

Smart Provisioning enhances day-to-day identity management operations when CA Identity Manager integrates with CA Identity Governance. When Smart Provisioning is enabled in an environment, certain tasks gain the following functionality:

- Suggested provisioning roles
- Out of Compliance violations

When CA Identity Manager administrators create a user, or modify a user, provisioning role, account, or account template, a request for a list of suggested roles or a request to validate changes for compliance violations is sent to CA Identity Governance. The CA Identity Governance Server evaluates the request against the existing role model or business policy rules (BPRs), and returns a list of suggested roles or any compliance violations to CA Identity Manager.

Important! You can implement Smart Provisioning in an Identity Manager Environment once you clean up the data (see page 50) in your CA Identity Governance universe and define the Business Policy Rules (see page 50) (BPRs) that you want to use for compliance.

Data Cleanup

When you initially import data into CA Identity Governance, the data may contain entities and relationships that cause violations. Pattern-based audit allows you to perform internal analytics to detect mistakes, such as a user that has too many resources compared to other users.

We recommend that you run a pattern-based audit check on imported data before you use Smart Provisioning in CA Identity Manager. This audit check cleans up your data so that fewer violations trigger when performing Smart Provisioning compliance checks in CA Identity Manager.

Note: For more information about pattern-based audit checks, see the *CA Identity Governance Client Tools Guide*.

Business Policy Rules (BPRs)

You can create Business Policy Rules (BPRs) for compliance checking in CA Identity Governance. These specific rules define constraints on user, role, and resource relationships, such as if you have X resource, you cannot have Y resource.

Once you create the BPRs you need for your business compliance needs, you list the BPRs you want to apply to a particular universe in the audit properties file. You specify the audit properties file to use when creating a universe. Once specified, this file defines the audit check parameters for the universe, regardless of what CA Identity Governance process kicks off the audit check.

When you have Smart Provisioning enabled in CA Identity Manager, the audit properties file defines which BPRs are used for Smart Provisioning compliance analytics.

Note: When you've completed all BPRs, you should run them against the imported CA Identity Manager configuration to be sure that the initial state of all CA Identity Manager users meets the compliance policies.

Edit Global Smart Provisioning Settings

To enable or disable Smart Provisioning functionality or edit global defaults for suggested roles and compliance checking across all tasks, log into the User Console as an administrator and go to System, CA Identity Governance Configuration, Define Configuration, and access the Smart Provisioning tab.

Note: If any task must be configured differently than the global settings, you can adjust the settings at the task level. Task-level settings override global settings.

You can edit the following Smart Provisioning settings:

Smart Provisioning Settings

Enable Smart Provisioning

Enables or disables Smart Provisioning functionality. Smart Provisioning can be disabled even though a connection with CA Identity Governance exists.

Global Tab Settings

Display Suggested Provisioning Roles Button

Determines whether the Suggested Provisioning Roles button appears on the Provisioning Roles tab.

Analytics Suggest Search Screen

Defines the search screen used for the role suggest feature.

Display Advanced Suggestion Configuration for Results

Determines whether the Advanced Suggestion Configuration section appears on the results page of the role suggest feature, after a search is performed.

The Advanced Suggestion Configuration section allows administrators to enter new criteria for a suggested roles search. Administrators can select the type of criteria (Matched Rule and Matched Attributes).

Enable 'Matched Rules' Analytics by Default

Determines whether CA Identity Manager suggests provisioning roles if the current user matches the rule that determines membership in a CA Identity Governance role.

You can override this default setting during the search using the Advanced Suggestion configuration screen.

Enable 'Matched Attributes' Analytics by Default

Determines whether CA Identity Manager suggests provisioning roles that other users who have similar profile attributes also have.

You can override this default setting during the search using the Advanced Suggestion configuration screen.

Display Weighted Score Column for 'Matched Attributes' Analytics

Determines the display of columns in the list of suggested provisioning roles. When this option is selected, CA Identity Manager displays the Weighted Score column, which indicates the highest score the suggested provisioning role received across all the criteria in the search.

Weighted Score Threshold for 'Matched Attributes' Analytics

Defines a threshold for 'Matched Attributes' search results returned by the suggest role feature. For each suggested role, CA Identity Governance returns a score from 1 to 100 percent depending on the level of attribute matching. Roles suggested with a score less than the threshold are not displayed.

Note: Some CA Identity Manager attributes may be more important to you than others, therefore CA Identity Governance allows you to customize the weight of any attribute in order to provide more useful analytics. For more information about setting attribute weights, see the *Configuration Guide*.

Bulk Loader Task Settings

Automatically Assign Roles that Match Rule

Determines if the Bulk Loader task uses ‘Matched Rules’ to search for roles. Any roles returned are automatically assigned.

Automatically Assign Roles that Match Attributes

Determines if the Bulk Loader task uses ‘Matched Attributes’ to search for roles. Any roles returned that exceed the Weighted Score Threshold are automatically assigned.

Weighted Score Threshold for 'Matched Attributes' Analytics

Defines a threshold for 'Matched Attributes' search results returned by the suggest role feature. For each suggested role, CA Identity Governance returns a score from 1 to 100 percent depending on the level of attribute matching. Roles suggested with a score less than or equal to the threshold are not assigned.

Note: Some CA Identity Manager attributes may be more important to you than others, therefore CA Identity Governance allows you to customize the weight of any attribute in order to provide more useful analytics. For more information about setting attribute weights, see the *CA Identity Governance Configuration Guide*.

Compliance Settings

Out of Compliance Analytics Level

Determines the level of information from the CA Identity Governance compliance analysis that CA Identity Manager displays.

You can set the following levels:

- No Analytics
- Issue Info Messages
- Issue Warning Messages
- Issue Error Messages

Note: For more information about the behavior of the different levels, see Types of Violations (see page 63).

Out of Compliance Severity Threshold

Indicates the minimum severity score of compliance violations to display. For example, if you specify 75, CA Identity Manager only displays compliance violations that have a severity score of 75 or above.

This setting limits the number of compliance violations that appear for the task.

If Issue Error Messages is selected, this setting also affects which tasks can be submitted. For example, if you set the cutoff to skip errors with low scores, users can submit tasks that contain errors.

Enforce Compliance Check on Submit

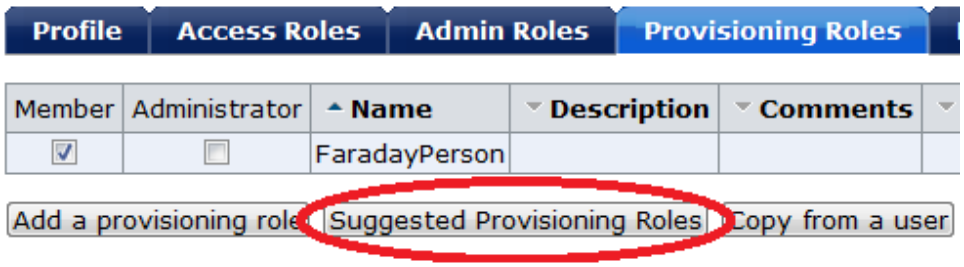
When selected, compliance checks occur automatically when a task is submitted. Users do *not* have to manually select the Check Compliance button to see compliance violations.

Note: If enabled, tasks executed by TEWS also enforce compliance checks on submit. This option does not apply to bulk loader tasks.

Suggested Provisioning Roles

When CA Identity Manager integrates with CA Identity Governance, CA Identity Manager can provide administrators with a list of provisioning roles that may be appropriate to assign to a user. CA Identity Governance determines the list of provisioning roles based upon criteria entered by the administrator.

By default, when an CA Identity Manager environment has an active connection to CA Identity Governance, the Provisioning Roles tab includes a Suggested Provisioning Roles button, as shown in the following graphic:



Administrators click the button to view the list of possible roles that they can assign to users. CA Identity Manager displays the list of roles that meet default criteria in a Provisioning Role search screen. This default criteria is defined when an administrator initially configures the search screen.

If administrators want to view additional provisioning roles, they can search for those roles without using the suggestion feature. In some implementations, administrators can also expand the Advanced Suggestion Configuration section to specify new suggestion criteria.

Note: In some implementations, the Advanced Suggestion Configuration is not available. System administrators can hide or show this section by selecting the Display Advanced Suggestion Configuration for Results option in the global default settings (see page 50).

Criteria for Suggested Roles

CA Identity Governance suggests provisioning roles for a user based on one or more of the following criteria:

- **Match Rule**

  CA Identity Governance suggests provisioning roles if the current user matches the rule that determines membership in the CA Identity Governance rule-based role.

  For example, the Sales Manager role has the following matching rule: Title = Sales Manager. If a user has Title=Sales Manager but is not a member of Sales Manager role, CA Identity Governance suggests this role for this user.

- **Match Attributes**

  CA Identity Governance suggests provisioning roles that belong to users with similar attributes.

  For example, an administrator wants to assign roles to an employee who has the following attributes in his profile:

  - Title: Sales Associate
  - Manager: Bob Folchart
  - Office: Northeast

  Users who have the same title, manager, and office have the Employee and Northeast Sales Associate roles. CA Identity Governance suggests these roles for assignment.

  CA Identity Governance calculates the probability that the suggested role is a match for the user by using the following criteria:

  - How closely the attributes from other users match the attributes of the current user
  - How many users with matching attributes have the role

  The best matches have the highest number of matching attributes *and* the largest number of users with the same role. For example, ten users who have the title Sales Associate and the Manager Bob Folchart have the Remote Employee role. Five users who are located in the Northeast office have the Quota-based Salary role. The Remote Employee role would receive a better match rating than the Quota-based Salary role.

View Suggested Roles

When CA Identity Manager integrates with CA Identity Governance, you can view a list of provisioning roles that CA Identity Governance suggests for a particular user. The provisioning roles that CA Identity Governance suggests meet the following criteria:

- You have privileges to assign the provisioning roles to the selected user.
- The provisioning roles match the search criteria (if any) that you enter in the Search field.
- The provisioning roles match at least one of the selected suggestions methods.

Follow these steps:

1. Execute a task in the User Console that includes the Provisioning Roles tab.

   By default, the Provisioning Roles tab appears in the Create User and Modify User tasks.

   CA Identity Manager displays any provisioning roles that the current user already has.

2. Click Suggested Provisioning Roles.

   A search screen, which allows you to specify criteria for the type of provisioning roles to suggest, opens.

   CA Identity Manager displays a list of provisioning roles that meet the default search criteria, which is defined in the global default settings (see page 50).

   Each provisioning role has a score (see page 57), which indicates how well the suggested role meets the specified criteria.

3. (Optional) Augment your search using one of the following methods:

   - To filter suggested provisioning roles based on an attribute of the role, such as name, enter criteria in the Search field.

     You can specify full or partial wildcard searches by using an asterisk (*) to represent all or part of a value.

   - To specify new matching criteria for suggested roles, expand the Advanced Suggestion Configuration section. Select the criteria (see page 54) to use in the search and click Suggest.

     CA Identity Manager returns a list of provisioning roles that meet the criteria you specified.

   Note: The Advanced Suggestion Configuration section may not available in all implementations. Administrators can choose to hide or show this section when they configure global default settings.

4. Select the roles that you want to assign to the user and click Submit.

   CA Identity Manager assigns the specified roles to the user.

Provisioning Role Scores

When CA Identity Manager displays suggested provisioning roles based on 'Matched Attributes' criteria, it may display the weighted score of each role, which indicates how well the suggested role meets the specified criteria. Higher scores indicate a better attribute match for the user receiving the provisioning roles.

Suggested role scores range from 1 to 100 percent, with 100 indicating the best match. CA Identity Governance generates the scores when it evaluates the criteria for suggested roles.

You can configure the score threshold that defines the cutoff for provisioning roles displayed. For example, you can specify that only suggested roles with a score of 90 or above are displayed.

A configuration option, which is available when you set global defaults (see page 50), determines the display of the score column.

Note: CA Identity Governance assigns default weights to all CA Identity Manager attributes. You can view these defaults under the Audit Properties screen in the CA Identity Governance Portal. You can assign higher or lower weights to certain attributes so that the Matched Attributes scores reflect the attributes that matter in your organization when searching for suggested roles. For more information about Audit Properties, see the *CA Identity Governance Configuration Guide*.

Add Suggested Roles to Users During a Bulk Loader Task

If you integrate CA Identity Manager with CA Identity Governance and have enabled Smart Provisioning in your CA Identity Manager Environment, you can configure the Bulk Loader task to retrieve and automatically add CA Identity Governance suggested roles to a user when it is run. For each user that is created or modified using the Bulk Loader, role assignments are suggested and compliance analytics are run. If the roles suggested are in compliance, the roles are assigned to the user.

When the Bulk Loader task completes, CA Identity Manager creates a Bulk Loader Notification for all certification managers. This notification appears under the Home tab and contains details on the Bulk Loader task. You can review the roles added to each user, or review any compliance violations that occurred. To resolve a compliance violation for a user, you can modify that user directly from the notification screen.

If the CA Identity Governance server is down when the Bulk Loader task runs, the users are created and modified, but no roles are assigned and no compliance checks are done.

To configure suggested roles for the Bulk Loader task, edit the following global Smart Provisioning settings (see page 50):

- Bulk Loader Task Settings
  - Automatically Assign Roles that Match Rule
  - Automatically Assign Roles that Match Attributes
  - Weighted Score Threshold for 'Matched Attributes' Analytics
- Compliance Settings
  - Out of Compliance Analytics Level
  - Out of Compliance Severity Threshold

Define Task-Level Settings for the Bulk Loader Task

While you can edit global defaults for all Smart Provisioning functionality, you may want to define alternate settings for the Bulk Loader task. Task-level settings override global default settings for Smart Provisioning.

To define task-level suggested roles defaults

1. Log into CA Identity Manager as an administrator who can modify admin tasks.
2. Select Roles and Tasks, Admin Tasks, Modify Admin Task.

   CA Identity Manager opens a screen where you can search for an admin task to modify.
3. Search for the Bulk Loader task you want to modify and click Select.
4. Click the Search tab.
5. Browse and Edit the Bulk Loader Search Screen.
6. Under CA Identity Governance Settings, select Use Task-Level Settings.

7. Edit the following task-level settings:

Automatically Assign Roles that Match Rule

Determines if the Bulk Loader task uses ‘Matched Rules’ to search for roles. Any roles returned are automatically assigned.

Automatically Assign Roles that Match Attributes

Determines if the Bulk Loader task uses ‘Matched Attributes’ to search for roles. Any roles returned that exceed the Weighted Score Threshold are automatically assigned.

Weighted Score Threshold for 'Matched Attributes' Analytics

Defines a threshold for 'Matched Attributes' search results returned by the suggest role feature. For each suggested role, CA Identity Governance returns a score from 1 to 100 percent depending on the level of attribute matching. Roles suggested with a score less than or equal to the threshold are not assigned.

Note: Some CA Identity Manager attributes may be more important to you than others, therefore CA Identity Governance allows you to customize the weight of any attribute in order to provide more useful analytics. For more information about setting attribute weights, see the *CA Identity Governance Configuration Guide*.

Out of Compliance Analytics Level

Determines the level of information from the CA Identity Governance compliance analysis that CA Identity Manager displays.

You can set the following levels:

- No Analytics
- Issue Info Messages
- Issue Warning Messages
- Issue Error Messages

Note: For more information about the behavior of the different levels, see Types of Violations (see page 63).

Out of Compliance Severity Threshold

Indicates the minimum severity score of compliance violations to display. For example, if you specify 75, CA Identity Manager only displays compliance violations that have a severity score of 75 or above.

This setting limits the number of compliance violations that appear for the task.

If Issue Error Messages is selected, this setting also affects which tasks can be submitted. For example, if you set the cutoff to skip errors with low scores, users can submit tasks that contain errors.

8. Click Ok.

   Task-level settings for the Bulk Loader task are saved.

Define Task-Level Settings for Suggested Roles

While you can edit global defaults for all Smart Provisioning functionality, you may want to define alternate settings for a specific CA Identity Manager task. Task-level settings override global default settings for Smart Provisioning.

To define task-level suggested roles defaults

1. Log into CA Identity Manager as an administrator who can modify admin tasks.
2. Select Roles and Tasks, Admin Tasks, Modify Admin Task.
3. Search for and select the task that you want to modify.
4. Click the Tabs tab.
5. Click the Edit icon next to the Provisioning Roles tab field.
6. Under Smart Provisioning Analytics Settings, select Use Task-Level Settings.
7. Complete the following fields as needed:

   Display Suggested Provisioning Roles Button

   Determines whether the Suggested Provisioning Roles button appears on the Provisioning Roles tab.

   Analytics Suggest Search Screen

   Defines the search screen used for the role suggest feature.

   Display Advanced Suggestion Configuration for Results

   Determines whether the Advanced Suggestion Configuration section appears on the results page of the role suggest feature, after a search is performed.

   The Advanced Suggestion Configuration section allows administrators to enter new criteria for a suggested roles search. Administrators can select the type of criteria (Matched Rule and Matched Attributes).

Enable 'Matched Rules' Analytics by Default

Determines whether CA Identity Manager suggests provisioning roles if the current user matches the rule that determines membership in a CA Identity Governance role.

You can override this default setting during the search using the Advanced Suggestion configuration screen.

Enable 'Matched Attributes' Analytics by Default

Determines whether CA Identity Manager suggests provisioning roles that other users who have similar profile attributes also have.

You can override this default setting during the search using the Advanced Suggestion configuration screen.

Display Weighted Score Column for 'Matched Attributes' Analytics

Determines the display of columns in the list of suggested provisioning roles. When this option is selected, CA Identity Manager displays the Weighted Score column, which indicates the highest score the suggested provisioning role received across all the criteria in the search.

Weighted Score Threshold for 'Matched Attributes' Analytics

Defines a threshold for 'Matched Attributes' search results returned by the suggest role feature. For each suggested role, CA Identity Governance returns a score from 1 to 100 percent depending on the level of attribute matching. Roles suggested with a score less than the threshold are not displayed.

Note: Some CA Identity Manager attributes may be more important to you than others, therefore CA Identity Governance allows you to customize the weight of any attribute in order to provide more useful analytics. For more information about setting attribute weights, see the *Configuration Guide*.

8. Click OK to return to the Tabs tab, then click Submit to save the task.

Compliance Violations

When CA Identity Manager integrates with CA Identity Governance, CA Identity Manager administrators can validate proposed changes against business policy rules in CA Identity Governance before committing changes. Validating changes before they are committed helps companies maintain the role model that they have defined for their operations.

Users can validate proposed changes involving users, roles, and accounts.

When Smart Provisioning is enabled for an environment, CA Identity Manager validates proposed changes to users, roles, and accounts before an administrator submits a task or approves a work item. The proposed changes are validated against Business Policy Rules (BPRs), which are defined in CA Identity Governance and represent various constraints on privileges. For example, a BPR may prevent users who have a purchasing department role, which allows members to order stock from subcontractors, from also having the subcontractor payment role. BPRs are created by a system administrator, business manager, auditor, or role engineer in CA Identity Governance.

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

You can configure CA Identity Manager to perform these validations automatically when users perform certain tasks, or allow users to initiate the validation manually.

Example: Compliance Violations

When support for compliance violations is enabled in an CA Identity Manager Environment, CA Identity Manager displays messages that indicate whether the proposed changes violate a compliance policy in CA Identity Governance.

In this example, the company has configured automatic compliance checks when administrators assign provisioning roles to employees.

An employee, Nancy McDonald, is moving from the Finance group to the Sales group. In the User Console, an administrator assigns the Sales Representative provisioning role to Nancy. This role gives role members access to sales applications that generate purchase orders.

Nancy also has the Finance provisioning role, which allows members to approve purchase orders. This role was assigned to Nancy when she first started at the company, but no longer applies in her new job.

The company has a business policy rule, defined in CA Identity Governance, which restricts users from having the Sales Representative and Finance roles at the same time. When the administrator attempts to submit the task that assigns the Sales Representative role to Nancy, an error message is displayed.

The administrator must remove the Finance role before assigning the Sales Representative role to Nancy. Once the violation is removed, the administrator can successfully submit the task.

Types of Violations

When compliance checks are performed, CA Identity Manager displays violation messages above the current task in the User Console. Violations can be one of the following categories:

- **Error**

  Indicates a severe compliance violation. Administrators cannot submit a task until the error is resolved.

- **Warning**

  Indicates a significant compliance violation. Administrators can submit a task with one or more warnings, however, they are prompted to confirm that they are overriding the warnings. This override becomes part of the permanent record of the task. Administrators can provide an optional justification, which is also recorded with the task history.

- **Alert**

  Indicates all other levels of compliance violations.

  Administrators can override alerts. No confirmation or justification is required.

Note: You configure the analytics level globally, or when you configure specific tasks that display compliance violations.

Compliance Violation History

When CA Identity Manager supports compliance violations, a record of all compliance checks is recorded in the task persistence database. Users can view this history by using the View Submitted Tasks task in the User Console.

If auditing is configured for the environment, CA Identity Manager also records compliance violations in the audit database.

CA Identity Manager records the following types of information in the compliance violation history:

- When compliance checks are performed
- Whether the checks are run manually or automatically
- The results of the compliance check
- Any errors or warnings that are encountered
- How many times the user alters proposed changes to clear an error
- Whether any warnings are ignored, and, if so, what justification is provided
- Whether any alerts are ignored

How to Configure Manual Validation

When manual validation is configured, a Check Compliance button appears on the task screen. Administrators can click the button to initiate a compliance or validation check before they submit a task. If the validation check returns an error message, the administrator must clear the violation before submitting the task.

Manual validation is the default method for compliance checking. Because administrators can choose to initiate a compliance check, there is minimal impact on system performance.

To configure manual validation checking, clear the Enforce Compliance Check on Submit check box when defining the global Smart Provisioning settings (see page 50) or the task-level settings (see page 60).

How to Configure Automatic Validation

You can configure critical tasks to always perform compliance checks by enabling automatic validation. In this case, CA Identity Manager performs the validation checks without requiring administrators to initiate the validation process.

Note: Automatic validation may affect performance. We recommend configuring automatic validation for critical tasks.

To configure automatic validation checking, select the Enforce Compliance Check on Submit check box when defining the global Smart Provisioning settings (see page 50) or the task-level settings (see page 60).

Define Task-Level Settings for Compliance Violations

While you can edit global defaults for all Smart Provisioning functionality, you may want to define alternate settings for a specific CA Identity Manager task. Task-level settings override global default settings for Smart Provisioning.

To define task-level compliance defaults

1. Log into CA Identity Manager as an administrator who can modify admin tasks.
2. Select Roles and Tasks, Admin Tasks, Modify Admin Task.
3. Search for and select the task that you want to modify.
4. Click the Tabs tab.
5. Click the Edit icon next to the tab controller selection field.

6. Under CA Identity Governance Settings, select Use task settings.
7. Complete the following fields as needed:

   Out of Compliance Analytics Level

   Determines the level of information from the CA Identity Governance compliance analysis that CA Identity Manager displays.

   You can set the following levels:

   - No Analytics
   - Issue Info Messages
   - Issue Warning Messages
   - Issue Error Messages

   Note: For more information about the behavior of the different levels, see Types of Violations (see page 63).

   Out of Compliance Severity Threshold

   Indicates the minimum severity score of compliance violations to display. For example, if you specify 75, CA Identity Manager only displays compliance violations that have a severity score of 75 or above.

   This setting limits the number of compliance violations that appear for the task.

   If Issue Error Messages is selected, this setting also affects which tasks can be submitted. For example, if you set the cutoff to skip errors with low scores, users can submit tasks that contain errors.

   Enforce Compliance Check on Submit

   When selected, compliance checks occur automatically when a task is submitted. Users do *not* have to manually select the Check Compliance button to see compliance violations.

   Note: If enabled, tasks executed by TEWS also enforce compliance checks on submit. This option does not apply to bulk loader tasks.
8. Click OK to return to the Tabs tab, then click Submit to save the task.

Smart Provisioning for the Bulk Loader Task

If you configure Smart Provisioning on the Bulk Loader task, you can retrieve and automatically add CA Identity Governance suggested roles to users when running the Bulk Loader. For each user that is created or modified using the Bulk Loader, role assignments are suggested and compliance analytics are run. If the roles suggested are in compliance, the roles are assigned to the user.

More information:

Add Suggested Roles to Users During a Bulk Loader Task (see page 57)

Chapter 6: Best Practices for Integration

This section contains the following topics:

Employ User ID to Specify User Managers

When you integrate CA Identity Manager with CA Identity Governance, employ the CA Identity Manager User ID to specify User Managers.

Import Primary Connector When Importing a New Endpoint

When you have a CA Identity Manager Connector defined in CA Identity Governance with a few endpoints, you have the option to add an additional endpoint later, after the original endpoints are already imported. You can also select only the new endpoint and import it without the others endpoints and without the primary (As Users) CA Identity Manager connector.

In this case, the data is imported correctly, but accounts are not matched to users. This issue occurs because the account mapping information comes from the primary connector. When importing a new endpoint defined as part of a CA Identity Manager connector, we recommend that you always import the primary (As Users) connector with the new endpoint.

Role Owner vs. Role Approver

In CA Identity Governance, you can select a CA Identity Manager provisioning role owner or role administrator as a CA Identity Governance certification approver. However, if you have a deployment with hundreds of owners for an CA Identity Manager role and you select role owner as the CA Identity Governance certification approver, CA Identity Governance sends an approval email to a limited number of owners. We recommend that you limit the number of role owners and role administrators set for a given role within CA Identity Manager.

imRole.approvers.countLimit

Defines the number limit of how many CA Identity Manager owners or administrators are notified during a certification.

Default: 20

Note: For more information about how to configure CA Identity Governance to retrieve CA Identity Manager Role Owners and Role Administrators, see the *CA Identity Governance Administration Guide*.

Define the %MANAGER% Well-Known

CA Identity Manager stores a user's manager information in DN format and has no reference to the name of the user's manager as it appears in the system.

For example, the user "John" has a manager field value of "cn=grali04,OU=development" in CA Identity Manager. This DN corresponds to the user "Linda", however there is nothing to indicate that "cn=grali04,OU=development" refers to this user.

When integrating with CA Identity Governance, and if the CA Identity Manager directory supports the %MANAGER% well-known on an attribute containing manager data, the CA Identity Manager directory attribute definition must define the well-known. Otherwise, CA Identity Governance can not find the manager information of employees for approvals during a certification, and sends the approval request to a default approver.

Note: For more information about well-known attributes, see the *CA Identity Manager Configuration Guide*.

Avoid Changing Attribute Mappings After Import

Avoid changing attribute mappings in connector configurations once you have run an initial import. If you do change the mapped attributes after initial import, it could cause significant performance impact, and you must run another import. However, CA Identity Governance cannot delete fields, so if you remove or rename a field, CA Identity Governance keeps the field with a blank value after the next import.

Provisioning Role and User Management

All provisioning roles and users imported into CA Identity Governance from CA Identity Manager must be managed through the Identity Manager User Console and *not* the Provisioning Manager. If you modify provisioning roles or delete users in the Provisioning Manager, you will not see those modifications in CA Identity Governance.

Compliance Best Practices

With the recent addition of Policy Xpress in CA Identity Manager, and now with the integration, you can set business compliance policies in different ways. When considering best practices, use the feature that allows for the greatest capabilities. We recommend the following:

- If you do not use Smart Provisioning in your CA Identity Manager Environment, you can set compliance policies for User Tasks as follows:
  - New deployments: Use Policy Xpress
  - Existing deployments: Use Preventative Identity Policies
- If you are using Smart Provisioning in your CA Identity Manager Environment, you can set compliance policies for User Tasks as follows:
  - Resource-level Segregation of Duties (SOD): Use CA Identity Governance Business Policy Rules (BPRs)
  - User attributes: Use Policy Xpress for new deployments, or Preventative Identity Policies for existing deployments.
  - Role Memberships: Use BPRs, Policy Xpress, or Preventative Identity Policies depending on preference.

The following table outlines requirements and capabilities for each CA Identity Manager compliance policy option:

Policy Option	Requires CA RCM and CA Identity Manager?	Scope of policy checking	Checks compliance against unmanaged endpoints?
Preventative Identity Policies	No	Roles	No
Business Policy Rules (BPRs)	Yes	Roles and Resources	Yes
Policy Xpress	No	Roles	No

FIPS Compliance

When integrating CA Identity Governance with CA Identity Manager, both systems must be FIPS-enabled, using the same FIPS key.

If both CA Identity Governance and CA Identity Manager systems are FIPS-enabled, any notifications that CA Identity Manager sends to CA Identity Governance using Continuous Update functionality is passed in clear text. To avoid sending information in clear text, set up SSL for both the CA Identity Governance system and the CA Identity Manager system.

Chapter 7: Troubleshooting

This section contains the following topics:

Smart Provisioning

Consider the following when troubleshooting Smart Provisioning functionality:

- Request ID

  The Request ID is a unique identifier that links a log message between CA Identity Manager and CA Identity Governance logs. This request ID is present in both sets of logs for a compliance or role suggest request sent from CA Identity Manager. The request ID has the following format:

  `[COMPLIANCE | SUGGESTROLES]-`*`envAlias-EventName-EventID`*

  Sample Request IDs for a Compliance and Suggest Request from CA Identity Manager are as follows:

  ```
  COMPLIANCE-sp8demo-Modify User-aa7f94f1-f75a95c3-65df7de6-bebf0cb
  SUGGESTROLES-sp8demo-Modify User-aa7f94f1-f75a95c3-65df7de6-bebf0cb
  ```

- View Submitted Tasks (VST): Compliance Messages

  All compliance violation messages sent from CA Identity Governance for a particular task (including bulk loader tasks) are recorded in VST.

- View Submitted Tasks (VST): Manage Bulk Loader Task Notifications
  - For details on this task, select the check box Show UnSubmitted Tasks during a VST search.
  - All details about the acknowledgment of the individual tasks associated with this bulk loader operation are in VST.
- Warning Messages for Role Suggest and Compliance

  CA Identity Manager displays warning messages under the following conditions when a role suggestion or compliance request is sent to CA Identity Governance:
  - Object is not Found in CA Identity Governance. The sample message displayed by CA Identity Manager is as follows: "The following user was not found in CA RCM: mabre01"
  - Object does not match CA Identity Governance filter. The sample message displayed by CA Identity Manager is as follows: "The following object does not match the filter in CA Identity Governance: babre01"
  - Account not assigned in CA Identity Governance. The sample message displayed by CA Identity Manager is as follows: "The following Account was not assigned to any user in CA RCM: taban01"

Continuous Update

Consider the following when troubleshooting Continuous Update functionality:

- View Submitted Tasks

  Event history contains a message "Changes associated with this event were successfully queued on the continuous update queue to be sent to CA Identity Governance".
- Request ID

  The Request ID is a unique Identifier that links a log message between CA Identity Manager and CA Identity Governance logs. This request ID is present in both sets of logs for a Continuous Update notification request sent from CA Identity Manager. The request ID has the following format:

  ```
  CONTINUOUSUPDATE-<envAlias>-<EventName>-<EventID>
  ```

A sample Request ID for a Continuous Update notification is as follows:

```
CONTINUOUSUPDATE-sp8demo-AssignProvisioningRoleEvent-4c8b83c4-75d52262-3e
883e88-2bf93853
```

- Log Messages related to the Analytics Queue
  - Log messages when the queue is being read.
  - Log messages when the Send Notifications is disabled.
  - Log messages when Send is Enabled.
  - Log messages when CA Identity Governance server is down.