CA Identity Manager
Provisioning Runbook for

ImageWare Systems, Inc.

Biometric Authentication Service

Legal Notice

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be disclosed by you or used for any purpose other than as may be permitted in (i) a separate agreement between you and CA governing your use of the CA software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and CA.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Table of Contents

Support

This document is produced by ImageWare Systems, Inc. (www.iwsinc.com or support@iwsinc.com), on behalf of CA Technologies Inc. (www.ca.com).

Contact CA Technologies

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

Product documentation feedback

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

For feedback or questions about ImageWare Systems, please contact support@iwsinc.com

Chapter 1: Introduction

Overview

The scope of this document is to provide the necessary steps required to configure the provisioning endpoint connection between CA Identity Manager 12.6, and the ImageWare Systems GMI Server endpoint.

The provisioning process

The endpoint provisioning process contains the following steps:

1. Install and configure the prerequisites
2. Configure provisioning for Identity Manager
3. Configure the Service Provider endpoint
4. Test the provisioned endpoint

CA prerequisites

- Install CA Identity Manager 12.6 Suite
- Configure user directory and provisioning directory
- Create an Identity Manager environment
- Import Roles and Tasks for SCIM endpoint types

ImageWare Systems, Inc. prerequisites for CA customers

In order to set up and use the ImageWare out-of-band biometric identity authentication component, there are a number of required prerequisites:

- Customer has established a tenant relationship with ImageWare Systems:
    - Either the customer has established a tenant relationship directly with ImageWare; *or*
    - The customer has attached themselves to CA Technologies as a tenant-client, using CA Technologies' tenant relationship with ImageWare Systems, Inc.
- Customer has established an appropriate client credential token for use in creating (provisioning) and removing (de-provisioning) users in the GMI system
- The ImageWare GMI system is setup for CA Identity Manager integration by configuring the GMI UserID attribute as immutable
- End-user is in possession of a mobile device that has either the GoVerifyID™ mobile application or a GoVerifyID-enabled application designated for providing biometric enrollment and verification through the GMI Server suite
- End-user has enrolled their biometrics to support future CA Identity Manager biometric identity verification requests

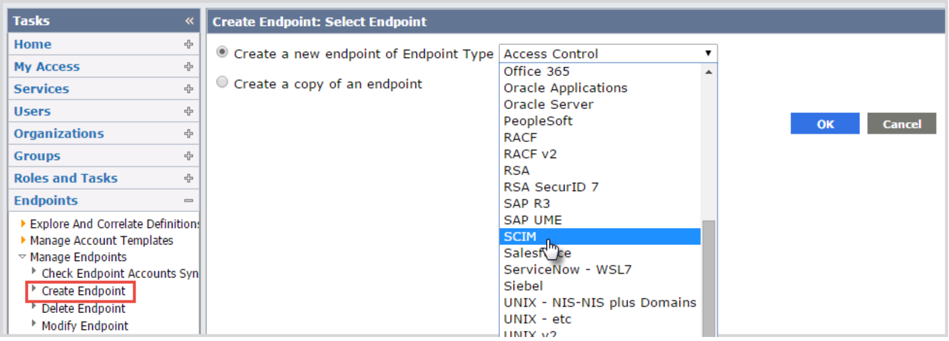
Chapter 2: Configure / provision CA Identity Manager (12.6)

Use the SCIM connector to acquire ImageWare Systems GMI Server endpoint

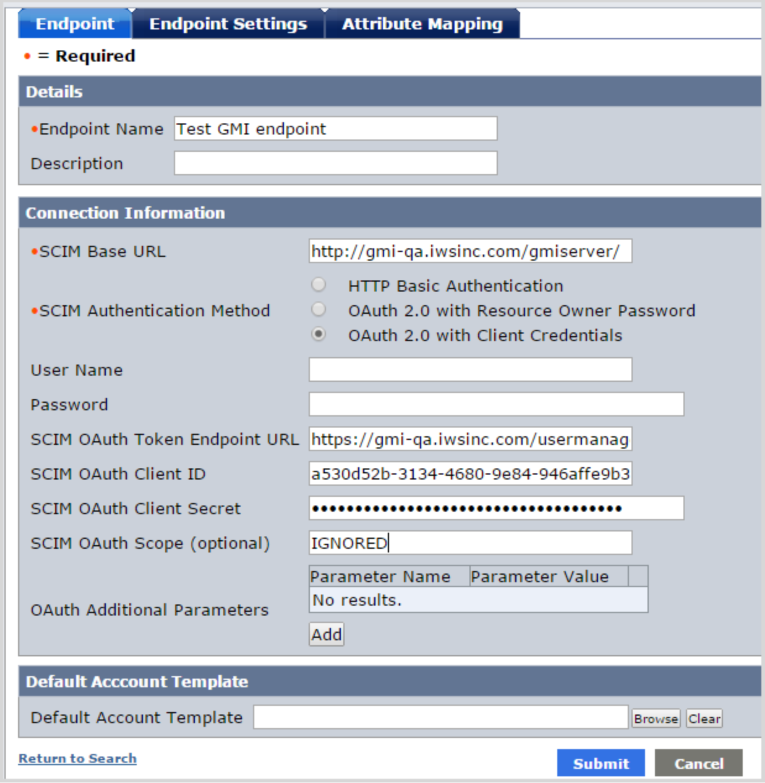
Create an endpoint

To acquire an endpoint:

1. Log in to *CA Identity Manager* and navigate to **Endpoints** → **Manage Endpoints** → **Create Endpoin**t.
2. Click the *Create a new endpoint of Endpoint Type* drop-down menu and select **SCIM**.



3. Click **OK**. The *Create SCIM Endpoint* form opens with the *Endpoint tab* open by default.



• = Required

Details

•Endpoint Name	Test GMI endpoint
Description	

Connection Information

•SCIM Base URL	http://gmi-qa.iwsinc.com/gmiserver/
•SCIM Authentication Method	○ HTTP Basic Authentication ○ OAuth 2.0 with Resource Owner Password ● OAuth 2.0 with Client Credentials
User Name	
Password	
SCIM OAuth Token Endpoint URL	https://gmi-qa.iwsinc.com/usermanag
SCIM OAuth Client ID	a530d52b-3134-4680-9e84-946affe9b3
SCIM OAuth Client Secret	••••••••••••••••••••••••••••••••••••
SCIM OAuth Scope (optional)	IGNORED
OAuth Additional Parameters	Parameter Name / Parameter Value No results. Add

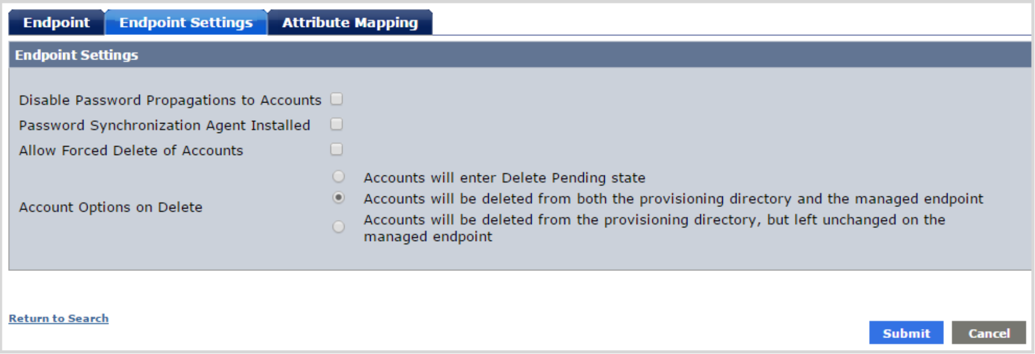
Default Acccount Template

Default Account Template	Browse Clear

4. Enter the following in the appropriate fields:

Field Name	Description
Endpoint Name	Name of your endpoint as you determine appropriate
Description	Optional
SCIM Base URL	https://<GMI_SERVER_FQDN>/gmiserver/v1
SCIM Authentication Method	OAuth 2.0 with Client Credentials
Username	N/A
Password / Confirm	N/A
SCIM OAuth Token Endpoint URL	https://<GMI_SERVER_FQDN>/usermanager/oath/token **NOTE:** *This field is required when the OAuth authentication method is selected*
SCIM OAuth Client ID	Relevant SCIM OAuth Client ID (this information is custom-defined for a partner and is available by contacting ImageWare Systems at support@iwsinc.com) **NOTE:** *This field is required when the OAuth authentication method is selected*
SCIM OAuth Client Secret	Relevant SCIM OAuth Client Secret (this information is custom-defined for a partner and is available by contacting ImageWare Systems, Inc. at support@iwsinc.com)
SCIM OAuth Scope	IGNORED, or some other string (optional) **NOTE:** *This field is required when the OAuth authentication method is selected*
OAuth Additional Parameters	None (optional)
Default Account Template	See *Explore and correlate definition*

5. Click the *Endpoint Settings tab*.



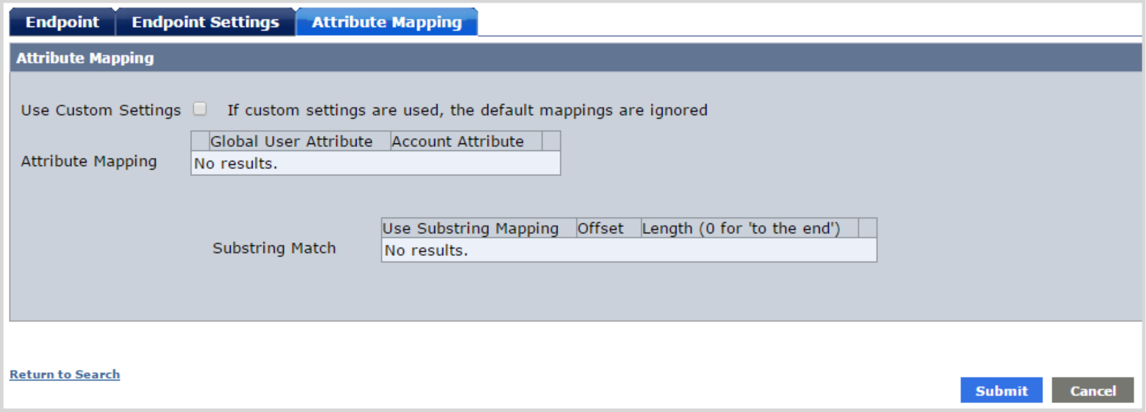
Endpoint Settings

Disable Password Propagations to Accounts □
Password Synchronization Agent Installed □
Allow Forced Delete of Accounts □

Account Options on Delete
○ Accounts will enter Delete Pending state
● Accounts will be deleted from both the provisioning directory and the managed endpoint
○ Accounts will be deleted from the provisioning directory, but left unchanged on the managed endpoint

NOTE: This tab is customized by CA or the relevant site or system administrator. Each setting is customized based upon the desired behavior regarding disabling and deleting accounts on the endpoint.

6. When any custom settings have been entered on this tab, click the *Attribute Mapping tab*.



Attribute Mapping

Use Custom Settings □ If custom settings are used, the default mappings are ignored

Attribute Mapping

Global User Attribute	Account Attribute
No results.	

Substring Match

Use Substring Mapping	Offset	Length (0 for 'to the end')
No results.		

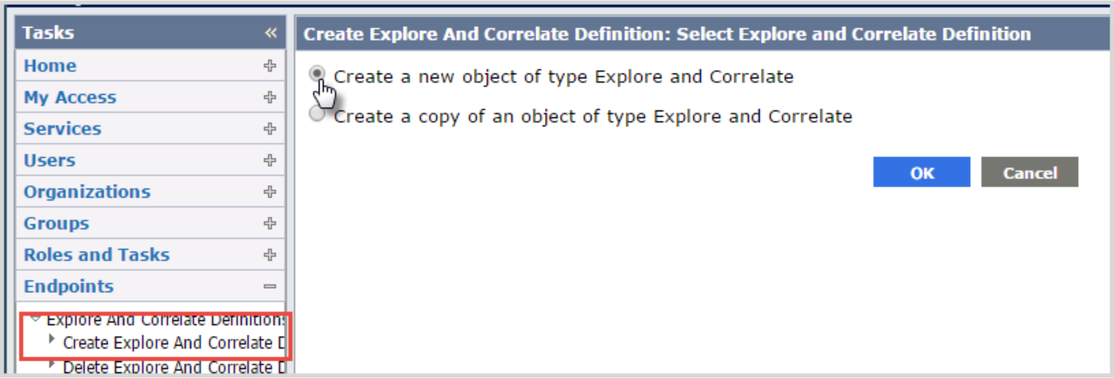
NOTE: This tab can be optionally changed if needed, but in most cases it is recommended that users keep the out-of-box mapping.

7. When any custom settings have been entered on this tab, click **Submit** to save all endpoint settings on the *Create SCIM endpoint* form.

Create an “explore and correlate” definition

To add users to an endpoint, you must create an “*explore and correlate*” definition for that endpoint. “*Explore*” identifies the accounts in the endpoint, and “*Correlate*” matches those accounts with either existing users in CA Identity Manager or creates those users / accounts.

1. Navigate to **Endpoints** → **Explore and Correlate Definitions** → **Create Explore and Correlate Definition**. A create new or create from copy form opens.

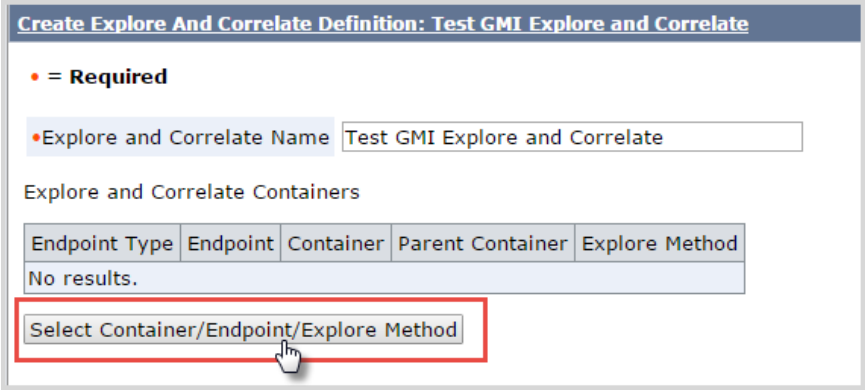

Tasks «
Home
My Access
Services
Users
Organizations
Groups
Roles and Tasks
Endpoints
Explore And Correlate Definitions
Create Explore And Correlate D
Delete Explore And Correlate D
OK
Cancel

Create Explore And Correlate Definition: Select Explore and Correlate Definition

● Create a new object of type Explore and Correlate

○ Create a copy of an object of type Explore and Correlate

2. Select **Create a new object of type Explore and Correlate** and then click **OK**. A *Create Explore and Correlate Definition* form opens.



Create Explore And Correlate Definition: Test GMI Explore and Correlate

• = **Required**

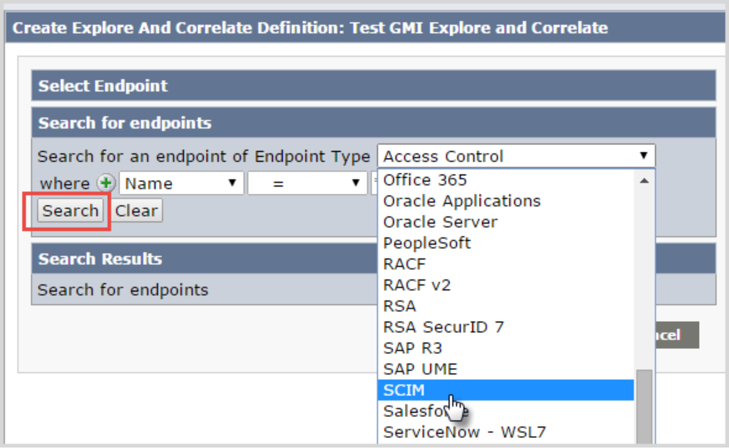
•Explore and Correlate Name: Test GMI Explore and Correlate

Explore and Correlate Containers

Endpoint Type	Endpoint	Container	Parent Container	Explore Method
No results.				

3. Enter an **Explore and Correlate Name** (this can be any string of text required).

4. Click Select Container/Endpoint/Explore method. A *Select Endpoint* form opens.



Create Explore And Correlate Definition: Test GMI Explore and Correlate

Select Endpoint

Search for endpoints

Search for an endpoint of Endpoint Type: Access Control

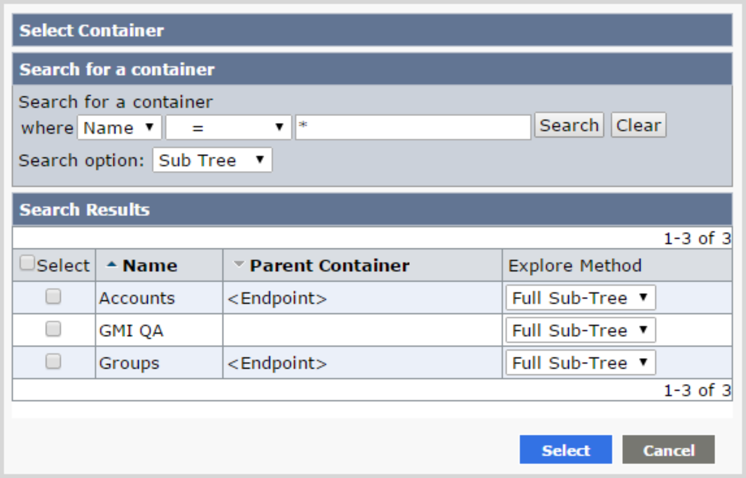
where Name =

Search Results

Search for endpoints

5. Click the *Search for an endpoint of Endpoint Type* drop-down menu and select **SCIM**.

6. **Search** for and **Select** the Endpoint created in *Endpoint creation*. A *Select Container* form opens.



Select Container

Search for a container

Search for a container

where Name = *

Search option: Sub Tree

Search Results

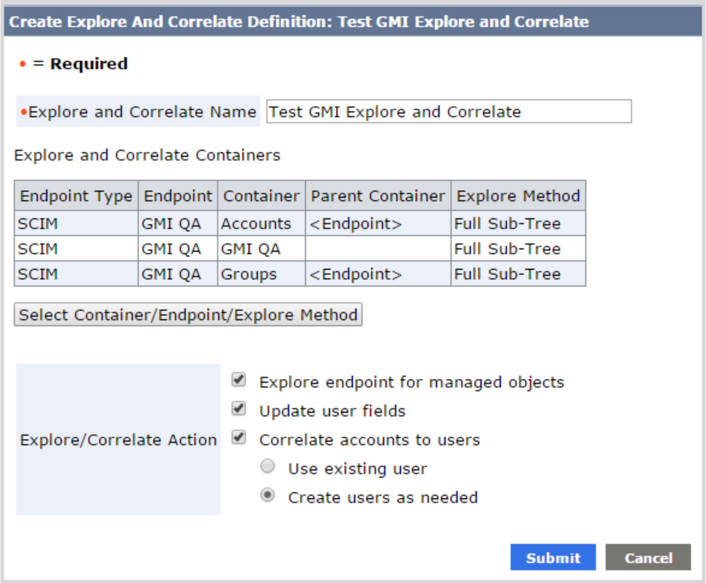
1-3 of 3

□ Select	Name	Parent Container	Explore Method
□	Accounts	<Endpoint>	Full Sub-Tree
□	GMI QA		Full Sub-Tree
□	Groups	<Endpoint>	Full Sub-Tree

1-3 of 3

7. Click **Search** and then place a checkmark next to the containers from which you wish to acquire data, such as Accounts, Groups, and so forth.

8. Click **Select**. The *Create Explore and Correlate Definition* form is now populated with the data you selected.



Create Explore And Correlate Definition: Test GMI Explore and Correlate

• = Required

•Explore and Correlate Name: Test GMI Explore and Correlate

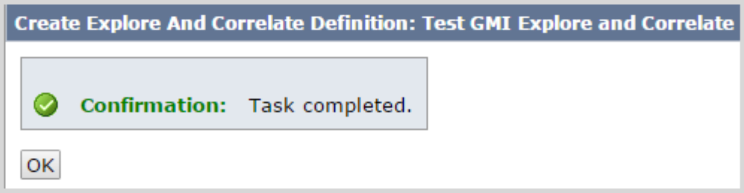
Explore and Correlate Containers

Endpoint Type	Endpoint	Container	Parent Container	Explore Method
SCIM	GMI QA	Accounts	<Endpoint>	Full Sub-Tree
SCIM	GMI QA	GMI QA		Full Sub-Tree
SCIM	GMI QA	Groups	<Endpoint>	Full Sub-Tree

Explore/Correlate Action:
☑ Explore endpoint for managed objects
☑ Update user fields
☑ Correlate accounts to users
○ Use existing user
● Create users as needed

9. Select the correct Explore and Correlate actions:
    - **Explore endpoint for managed objects**
    - **Update user fields**
    - **Correlate accounts to users → Create users as needed**

10. Click **Submit**. A confirmation window should open.



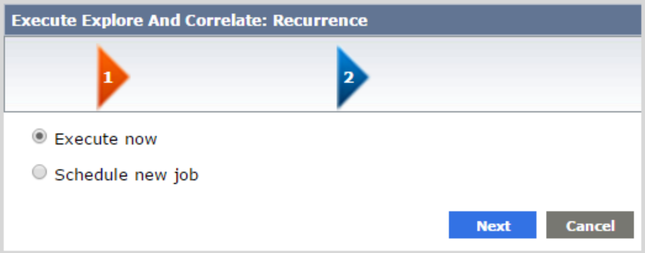
Create Explore And Correlate Definition: Test GMI Explore and Correlate

Confirmation: Task completed.

11. Click **OK**.

12. Click **Endpoints → Execute Execute Explore and Correlate**.

13. Select **Execute Now** and then click **Next**.



Execute Explore And Correlate: Recurrence

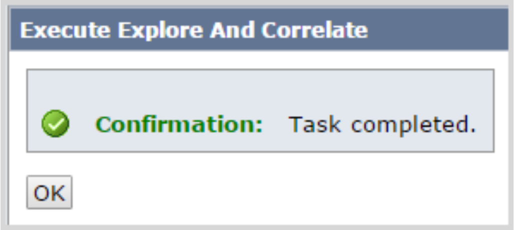
● Execute now
○ Schedule new job

14. Click **Browse** to locate the *Explore and Correlate definition* created in this section. A *Select Explore and Correlate Definition* form opens.

15. Click **Search**. A list of possible explore and correlate definitions opens.

16. Select the correct *Explore and Correlate Definition* and then click **Select**.

17. Click **Finish** to begin execution. A confirmation window should open.



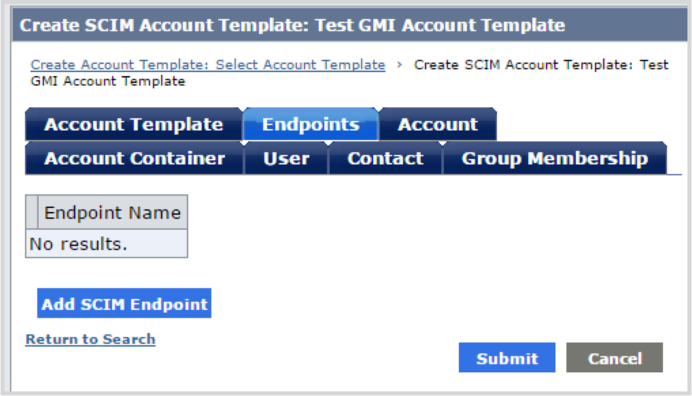
Execute Explore And Correlate

Confirmation: Task completed.

Create account templates

To simplify account management, the recommended best practice is to create and maintain accounts using Account Templates, which are then used in provisioning Roles. Standardizing account maintenance through templates allows the administrator to control which account attributes are affiliated with which Endpoints when user accounts are created.

1. To create an account template, navigate to **Endpoints** → **Manage Account Templates** → **Create Account Template**. A *Create Account Template* form opens.
2. Click the *Create a new account template of Endpoint Type* drop-down menu and select **SCIM**.
3. Click **OK**. The *Create SCIM Account Template* form opens with the *Account Template* tab opened by default.
4. Enter an **Account Template Name**. This field can be named anything you determine appropriate.
5. Click the *Endpoints tab*.



Create SCIM Account Template: Test GMI Account Template

Create Account Template: Select Account Template › Create SCIM Account Template: Test GMI Account Template

Endpoint Name
No results.

6. Click **Add SCIM Endpoint**. The *Find Endpoints* search form opens.

7. **Search** for and **Select** the Endpoint created in *Endpoint creation*. The Create SCIM Account Template now contains the selected endpoint.
8. In regard to the *Account*, *Account Container*, *User*, *Contact*, and *Group Membership* tabs:
   - *Account*, *User*, and *Contact* mapping can be modified as needed, but in most cases the default values should be used, for example use the ***%AC% (Account Name)*** rule string for the *User Name* attribute. The user name value must be maintained over the life of the provisioned account and therefore must be an immutable attribute like the account name.

> **NOTE:** For demonstration purposes in GoVerifyID, the email address is used for account name—this is what the GoVerifyID application requires during registration. It is expected that integration with an existing Identity Manager will involve synchronizing this user name value between Identity Manager and the customized GoVerifyID application; an appropriate user profile attribute should be chosen.

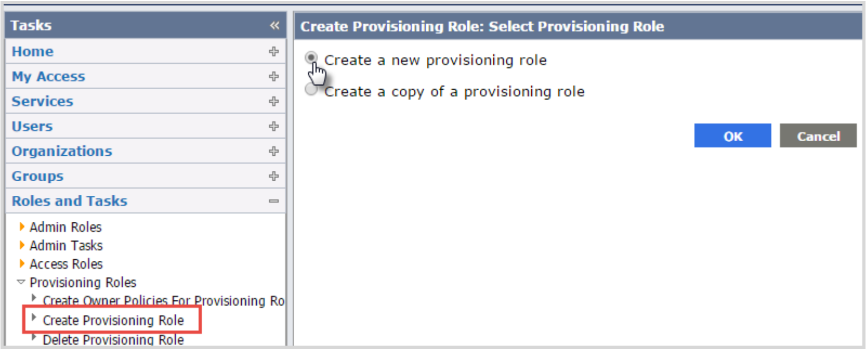
   - *Account Container* tab should remain unchanged
   - *Group Membership* can be optionally configured
9. When you have completed any additional changes to these tabs, click **Submit**.

   A *Confirmation message* should open. Click **OK**.

Create a provisioning role

A provisioning role contains one or more account templates. When you apply that role to a user, the user receives the accounts that were previously defined by the templates.

1. To create a provisioning role, navigate to **Roles and Tasks** → **Provisioning Roles** → **Create Provisioning Role**. A *Create new* or *Create from copy* form opens.



Create Provisioning Role: Select Provisioning Role

● Create a new provisioning role

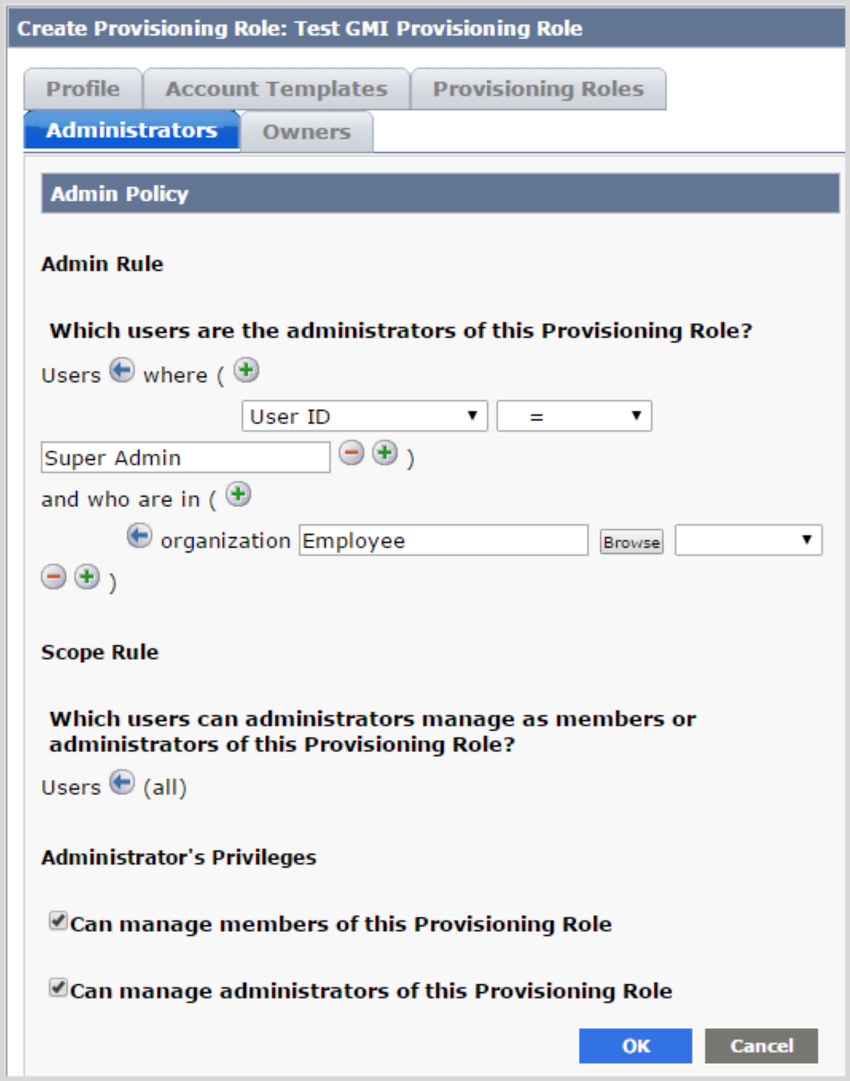
○ Create a copy of a provisioning role

2. Select **Create a new provisioning role** and then click **OK**. A *Create Provisioning Role* form opens with the *Profile tab* opened by default.
3. Enter a **Profile Name**. This field can be named anything you determine appropriate.
4. Click the *Account Templates tab*.

5. Click **Add Account Template**. The *Select Account Template* search form opens.
6. From the *Search for an account template of Endpoint Type* drop-down menu, select **SCIM**.
7. **Search** for and **Select** the account template created in Create account templates. The *Create Provisioning Role form → Account Templates tab* now contains the selected account template.
8. Do not make changes to the *Provisioning Roles tab*.
9. Click the *Administrators tab*.

   Administrators can add and remove members of the provisioning role.
10. Click **Add**. The *Admin Policy form* opens.

    On this form, you can select from a variety of parameters to create administrator roles, privileges, scope, and ownership levels. Set the rules and guidelines that establish the users who will be administrators of this provisioning role, and which users they can manage. When you have completed adding administrator users, click **OK**.



Create Provisioning Role: Test GMI Provisioning Role

Admin Policy

Admin Rule

Which users are the administrators of this Provisioning Role?

Users where (

User ID =

Super Admin)

and who are in (

organization Employee Browse

)

Scope Rule

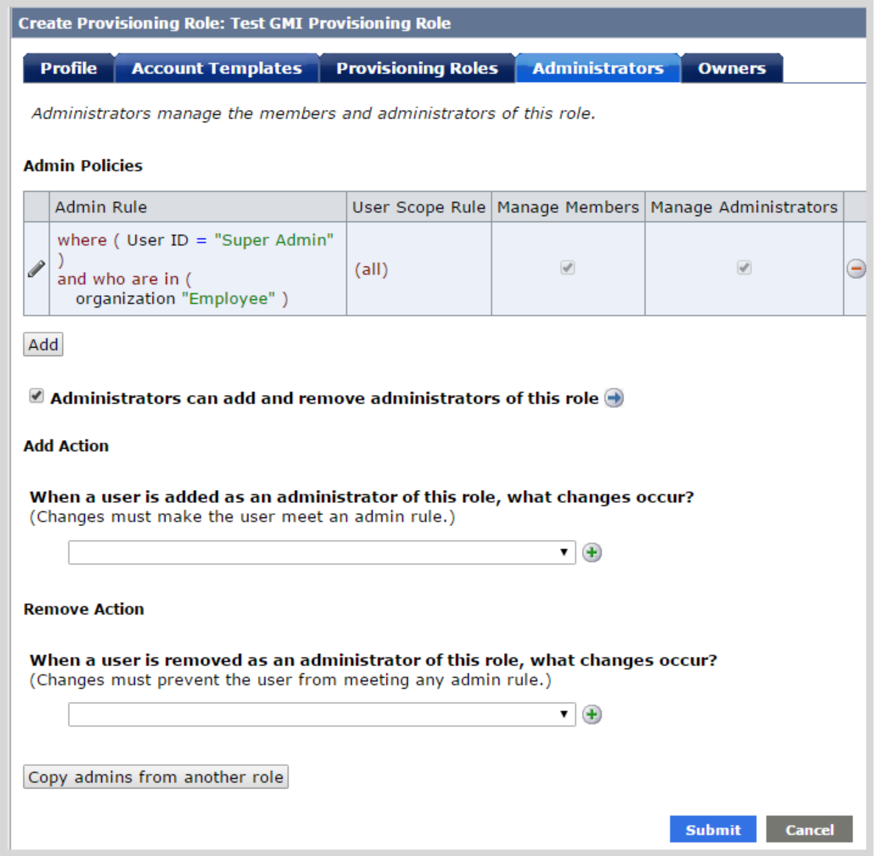
Which users can administrators manage as members or administrators of this Provisioning Role?

Users (all)

Administrator's Privileges

☑ Can manage members of this Provisioning Role

☑ Can manage administrators of this Provisioning Role



Create Provisioning Role: Test GMI Provisioning Role

Administrators manage the members and administrators of this role.

Admin Policies

Admin Rule	User Scope Rule	Manage Members	Manage Administrators
where (User ID = "Super Admin") and who are in (organization "Employee")	(all)	☑	☑

☑ **Administrators can add and remove administrators of this role**

Add Action

When a user is added as an administrator of this role, what changes occur?
(Changes must make the user meet an admin rule.)

Remove Action

When a user is removed as an administrator of this role, what changes occur?
(Changes must prevent the user from meeting any admin rule.)

11. Click the *Owners tab*.

    Owners are users who can modify and delete the provisioning role.

12. Click **Add**. The *Owner Rule form* opens.

    On this form, you can establish the rules for which users will be owners of this provisioning role. When you have completed adding owner users, click **OK**.

13. Click **Submit** to complete adding this provisioning role.

    A *Confirmation message* should open. Click **OK**.

Set up Policy Xpress

Policy Xpress is used to create complex business logic (or policies) in CA Identity Manager without developing custom code. This tool can automate endpoint provisioning by assigning the appropriate Provisioning Role(s) whenever a new User is created.

1. Navigate to **Policies** → **Policy Xpress** → **Create Policy Xpress Policy**.

2. Select **Create a new object** of type **Policy Xpress**.

3. On the **Profile** tab:
   a. Complete all fields, selecting **Submitted Task** as the Policy Type.
   b. Provide a **Category Name** or select one from the list.

4. On the **Events** tab:
   a. Select **Task Started** as the *Event State*
   b. Select **Create User** as the *Event Name*

5. On the **Action Rules** tab:
   a. Add **Action when Matched**
      - **Category:** *Roles*
      - **Type:** *Set Provisioning Role*
      - **Function:** *Add*
      - **Provisioning Role Name:** *Select the provisioning role for your endpoint*

6. To test:
   a. Navigate to **Users** → **Manage Users** → **Create User** and then create a new user
   b. From the endpoint user interface, verify that the new user was automatically created on the correct endpoint.

NOTE: For more information on how to create Policy Xpress Policies, refer to the ***Policy Xpress*** section of the *CA Identity Manager* documentation. This can be found at https://wiki.ca.com.

Chapter 3: Configure the ImageWare Systems GMI Server endpoint

Connect with ImageWare Systems, Inc.

Follow the steps given below to configure the ImageWare Systems GoMobile Interactive (GMI) Server endpoint:

1. Contact ImageWare Systems Support team (support@iwsinc.com) to begin the process of setting up the ImageWare Systems GMI Server. The sections in this chapter provide a general overview of what this process entails for business partners (called **Tenants**) such as CA Technologies.

2. See the *ImageWare Systems, Inc. prerequisites for CA customers* section of this document.

Tenant requirements

Tenants who use ImageWare's *GoVerifyID client application or service* and / or *GMI server application layer* will need to remain aware of the following requirements:

- Tenants must establish a tenant relationship with ImageWare and use the methods provided by ImageWare to engage with ImageWare's GMI server app layer.
- GMI Server API are implemented via RESTful HTTP calls over SSL. Responses are JSON-encoded. Each API REST call made by tenant's servers must contain an authenticated client or resource owner OAuth 2.0 bearer token generated using credentials provided by ImageWare for each tenant installation.
- Tenants are further responsible to provision their authorized end-users through the GMI Server API or the GMI Admin Portal (a web-based interface for managing Tenant accounts).

ImageWare requirements

ImageWare will:

- Create the tenant's profile on ImageWare servers.
- Create an OAuth 2.0 client credential used by the tenant to access ImageWare GMI Server application layer and utilize the GMI Server API from the tenant's client servers.
- Work with representatives from the tenant to establish Administrative user roles for both GMI Server and the GMI Admin Portal.

ImageWare System’s GMI Admin Portal

When Tenants establish a relationship with ImageWare Systems, Inc., they are given the GMI Server SDK containing all relevant API, and also are provided with a login identity to the *GMI Admin Portal*. This Admin Portal is a web interface created for ImageWare’s Tenants, and is used by the Tenant’s administrative users to manage the following:

- Their own **Tenant account**
- Any **end-users** attached to their account, as well as a mechanism to manage end-user’s:
  - **Messages**; and
  - **Devices***
- Their own **system administrator credentials***
- Their own **client server credentials***; and
- Any **applications*** or services they use to communicate with end-users

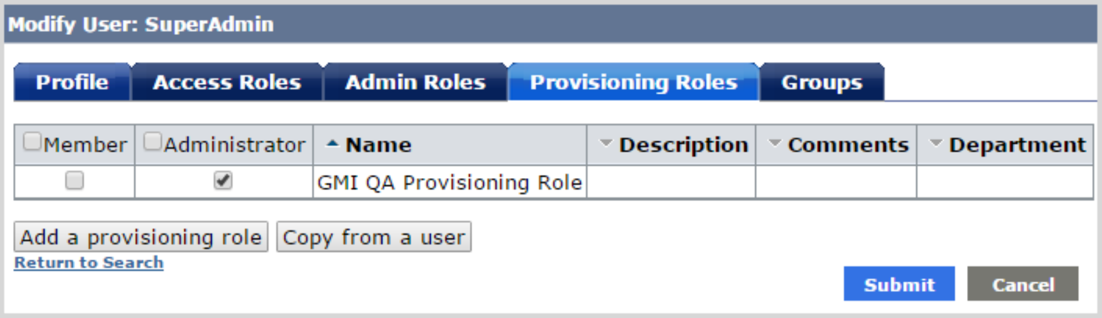
Some additional, useful features include the ability to push ad-hoc messages to end-users, review end-user statuses at-a-glance, bulk upload and download user lists, run reports on activity, and add or delete credentials, users, and other required information in a real-time, easy-to-use environment.

***NOTE:** Not all tenants have been given access to all GMI Admin Portal rights and capabilities. Depending upon your designated administrative user role, you might not see all of the features described in this section when using the GMI Admin Portal.

Chapter 4: Test provisioning to the GMI Server endpoint

Provision a user

1. To provision a user in CA Identity Manager, navigate to **Users** → **Manage Users** → **Modify User**. The *Search for a user* form opens.
2. **Search** for and **Select** the User you wish to provision to the GMI endpoint. The *Modify User* form opens, with the *Profile tab* opened by default.
3. Enter or modify any of the fields on this tab as appropriate.
4. Click the *Provisioning Roles tab*. Existing users are listed on this tab.
5. Click **Add a provisioning role**. The *Search for a provisioning role* form opens.
6. **Search** for and **Select** the provisioning role you created in *Provisioning Role*. The *Modify User form, Provisioning Roles tab* now contains the selected user role.
7. Check **Member** and/or **Administrator** checkboxes for this provisioning role
8. Click **Submit**. A Confirmation message should open. Click **OK**.



Modify User: SuperAdmin

□Member	□Administrator	▲ Name	▼ Description	▼ Comments	▼ Department
□	☑	GMI QA Provisioning Role			

Modify a user

GMI does not store Personally Identifying Information (PII) for individual users. The only data shared between CA Identity Manager and GMI is the `User Name` value defined in *Create account template*. The User Name value is immutable, therefore user modification is not supported, nor necessary, for CA Identity Manager provisioning to GMI.

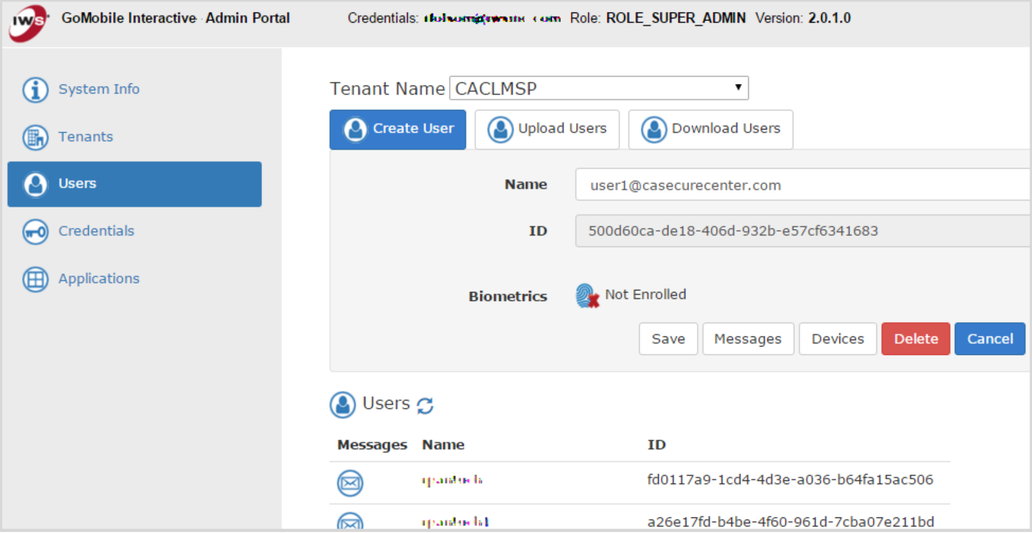
Deprovision a user

1. To deprovision a user in CA Identity Manager, navigate to **Users** → **Manage Users** → **Modify User**. The *Search for a user* form opens.
2. **Search** for and **Select** the User you wish to deprovision from the GMI endpoint. The *Modify User* form opens, with the *Profile tab* opened by default.
3. Click the *Provisioning Roles tab*. The selected user should be shown on this tab.

4. De-select the **Member** or **Administrator** checkbox for this user to deprovision them from the endpoint.
5. Click **Submit**. A Confirmation message should open. Click **OK**.

Confirm that user was provisioned or deprovisioned in the GMI Admin Portal

Once you have provisioned (or deprovisioned) an end-user in CA Identity Manager, you can confirm that the user has been added or removed as an end-user attached to your Tenant account in the GMI Admin Portal by navigating to the *GMI Admin Portal, Users tab* and performing a Search <Ctrl+F> or by browsing through the list of existing users attached to your Tenant account in the Users table.



Credentials: [illegible] Role: ROLE_SUPER_ADMIN Version: 2.0.1.0

Tenant Name CACLMSP

Name user1@casecurecenter.com

ID 500d60ca-de18-406d-932b-e57cf6341683

Biometrics Not Enrolled

Users

Messages	Name	ID
✉	[illegible]	fd0117a9-1cd4-4d3e-a036-b64fa15ac506
✉	[illegible]	a26e17fd-b4be-4f60-961d-7cba07e211bd

Chapter 5: Exception Handling

The following troubleshooting tips may be helpful to keep in mind during setup:

- The client credentials must be valid for the GMI server SCIM endpoint.
- In order to correctly provision a user, the user must not already exist on the GMI server.
- User names must be unique, therefore an email address or similar identifier is suggested.
- The Identity Manager User-User Name attribute value must be identical to the User-User Name value the person uses when registering themselves with the appropriate GoVerifyID or GoVerifyID-compatible application.

Chapter 6: Summary

The following is a summary of key steps in the Identity Manager provisioning setup process.

1. Configure ImageWare Systems’ GMI Server tenant to represent the CA Identity Manager user base.
2. Gather the client credentials and GMI Server SCIM endpoint details for use in configuring CA Identity Manager.
3. Using CA Identity Manager's administrative user interface, create the appropriate SCIM endpoint and associated Account Template and Provisioning Role to define provisioning from Identity Manager to GMI Server.

Appendices: CA Scalability Testing

Appendix A: Testing Checklist

Scalability testing performed with test servers at CA in conjunction with the GMI SCIM interface:

Test Name	Complete	# Users	Time	Result/Comments
Explore and Correlate against Endpoint	□	250,000	~6 hours	250,000+ users successfully correlated to CA IM.
Bulk Load - Provisioning Create Users	□	10,000	~1 hour	7 of total were not provisioned in CA IM and correctly not provisioned in GMI. All others successfully provisioned.
Bulk Load - Provisioning Modify Users	□			N/A. GMI does not have any attributes for Person Identity that can be modified.
Bulk Load - Provisioning Delete Users	□	1,000	minutes	All users successfully deleted.
Special Character Testing (See Appendix B)	□			
Additional CRUD Testing (See Appendix C)	□			

Appendix B: Special Character Testing

- □ Create Users in IM with Special Characters in the fields that will be provisioned to the endpoint.
- □ Make sure to test users with the following characters: , \ / ! @ # $ % & * ( ) - _ + = ` " : ; [ ] { } < > ^ ~ . ? |
  - **The GMI System has a more limited set of special characters supported for User ID (which is the only field provisioned from CA to GMI). Those characters are @ . _**
- □ Provision, Update, and De-Provision those users to the endpoint.
  - **Tested successfully.**

Appendix C: Additional CRUD Testing

In addition to previous Create, Read, Update, and Delete (CRUD) testing that has been completed, it is important to also test the following as it applies to your endpoint:

- □ **Delete and recreate the same users**. Ensure that users are deleted and recreated properly on the endpoint.
  - **Tested successfully**.
- □ **Lock and suspend users**. Ensure that these attributes are set properly on the endpoint.
  - **This does not apply to GMI System integration**.

> **NOTE:** This does not apply to GMI System integration because locked and suspended users are managed by CA Identity Manager, the SSO system, or other CA software. GMI provides user biometric identity validation and authentication or rejection to CA. CA is responsible for granting the user access to appropriate applications based upon their permissions, specifically user status (active, locked, or suspended).

- **Password changes**, including *must change on next login*, and *password expired*. Ensure that the password is reset and that these attributes are set properly on the endpoint.
  - **This does not apply to GMI System integration**.

> **NOTE:** This does not apply to GMI System integration because password policies and rules are managed by CA Identity Manager, the SSO system, or other CA software. GMI provides user biometric identity validation and authentication or rejection to CA. CA is responsible for granting the user access to appropriate applications based upon their permissions, specifically the user's password policies.

- **Relationship associations between primary object and secondary object** (i.e. account/group). Ensure that these relationships are set and removed properly on the endpoint.
  - **This does not apply to GMI System integration**.

> **NOTE:** This does not apply to GMI System integration because primary and secondary objects (such as accounts and groups) are managed by CA Identity Manager, the SSO system, or other CA software. GMI provides user biometric identity validation and authentication or rejection to CA. CA is responsible for granting the user access to appropriate applications based upon their permissions, specifically permissions related to their group membership(s).
>
> It is important to also note that GMI does not manage or make use of groups. Groups and group membership are entirely the responsibility of CA / CA software.