CA CloudMinder™

Getting Started with Identity Management

1.53

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.

CA Technologies Product References

This document references the following CA Technologies products:

- CA CloudMinder™ Identity Management
- CA CloudMinder™ Advanced Authentication
- CA CloudMinder™ Single Sign-On
- CA Directory
- CA IdentityMinder™
- CA AuthMinder™
- CA RiskMinder™
- CA SiteMinder®
- CA SiteMinder® for Secure Proxy Server
- CA Layer 7

Contents

Chapter 1: Getting Started with Identity Management

This section contains the following topics:

Connecting to Endpoints

For information on connectors, connector servers, and connecting to endpoints, see CA Identity Management and Governance Connectors.

It includes instructions for the the following connectors:

CA ACF2

CA Strong Authentication

CA Privileged Identity Manager

CA Data Protection

CA Single Sign-On Connector for Advanced Policy Server

CA Top Secret

Dynamic Connectors (Connector Xpress)

Google Apps

Google Apps CA API Gateway Connector

IBM DB2 for z/OS

IBM DB2 UDB

IBM i5/OS (OS/400)

IBM RACF

Lotus Notes Domino

Microsoft Active Directory, Microsoft Exchange, and Microsoft Lync

Microsoft Azure

Microsoft Office 365

Microsoft SQL Server

Microsoft Windows

Oracle Applications Connector

Oracle PeopleSoft

Oracle Siebel CRM

RSA ACE SecurID Connector

RSA SecurID 7 Connector

Salesforce

SAP

SCIM

ServiceNow

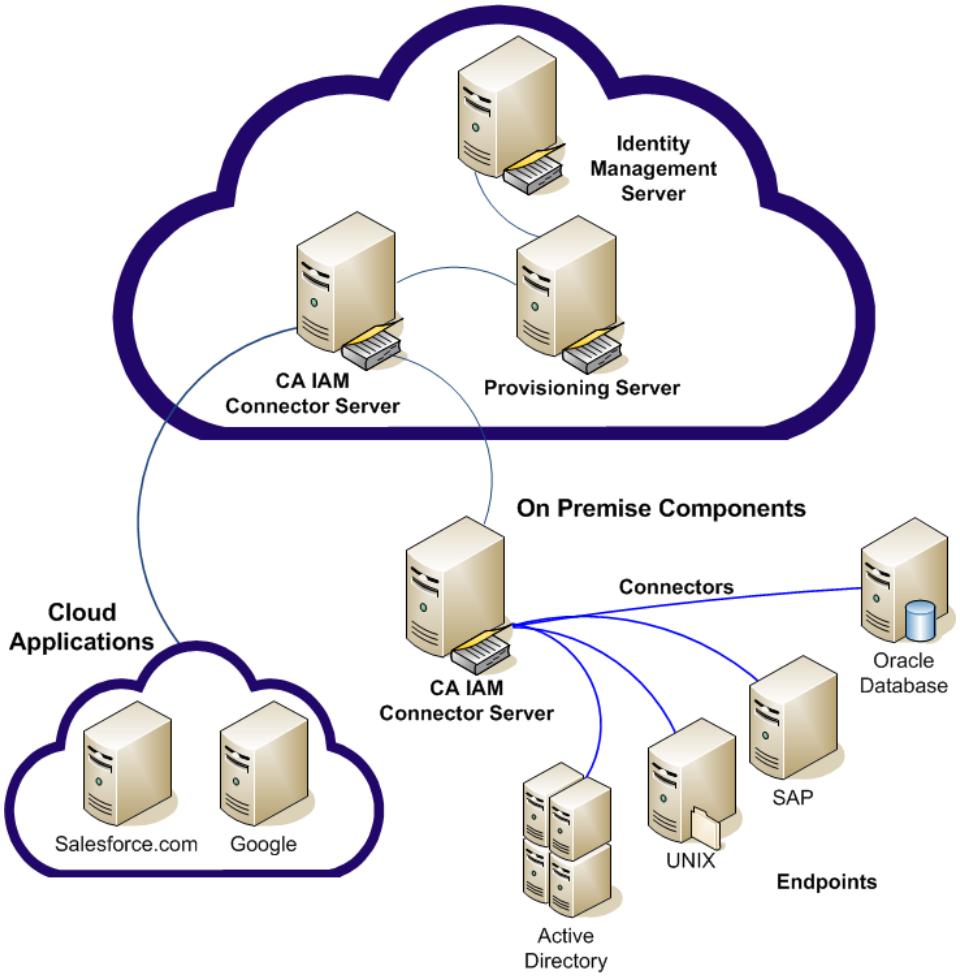
UNIX

Web Services

Zendesk

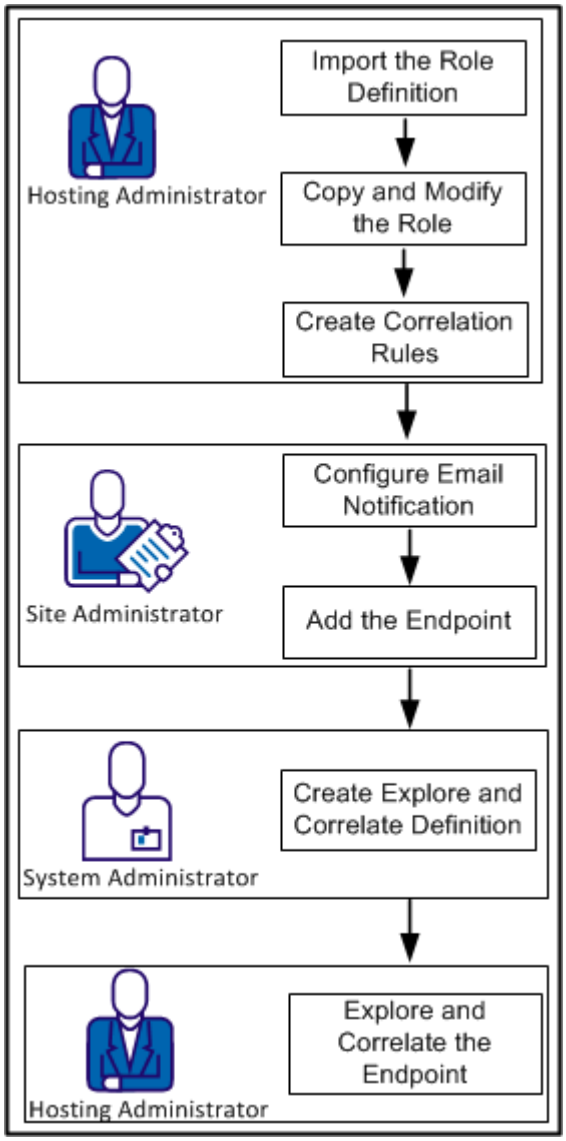
Integrating Managed Endpoints

With Identity Management, you can manage accounts on multiple systems from a single user interface, the User Console. The accounts are on systems that are referred to as managed endpoints, or simply endpoints. In the following example, you manage users on two cloud endpoints and four on-premise endpoints. You can assign accounts on any combination of endpoints to a user. When you integrate the endpoint, Identity Management associates each endpoint account with a user in the provisioning directory.



Integrating a managed endpoint is a multi-step process as follows and involves different administrators.

Equation 1: Steps to integrate a new endpoint



The following procedures describe how to integrate endpoints, so that endpoint accounts can be managed from the User Console.

1. Import the Role Definition File (see page 12)
2. Copy and Modify the Role (see page 13)
3. Create Correlation Rules (see page 14)
4. Configure Email Notification for the Endpoint (see page 16)
5. Add the Endpoint to the Environment (see page 16)
6. Create an Explore and Correlate Definition (see page 17)
7. Explore and Correlate the Endpoint (see page 19)

Import the Role Definition File

You import the role definitions from a file that applies to the new endpoint. This procedure requires access to the Management Console.

Follow these steps:

1. From the Management Console, click Environments.
2. Select the environment where you are adding the endpoint.
3. Click Role and Task Settings.
4. Click Import.
5. Select an endpoint under Endpoint Type.
6. Click Finish.

   The status of the import appears in the current window.
7. Click Continue to exit.
8. Restart the environment so that the changes take effect.

Copy and Modify the Role

Follow these steps:

1. Create a role as a copy of the imported role.
2. Name the new role: *Endpoint-Name* Tenant Provisioning Manager Role.
3. Modify the original Endpoint-Name Provisioning Manager Role as follows:
   a. Click the Members tab.

      Note that the member policy is set to System Manager.

   b. Change the policy to include only users who are members of the CSP Administrator role.
4. Modify the Endpoint-Name Tenant Provisioning Manager role as follows:
   a. Click the Members tab.

      Note that the member policy is set to System Manager.

   b. Change the policy to include only users who are members of these roles:

      CSP Administrator

      MSP Administrator

      Tenant Administrator

   c. Verify that new role omits the following tasks:

      Create Account Template

      Create Endpoint

      Create Explore And Correlate Definition

      Delete Account Template

      Delete Endpoint

      Delete Explore And Correlate Definition

      Execute Explore And Correlate

      Manage Orphan Accounts

      Manage System Accounts

      Modify Account Template

      Modify Endpoint

      Modify Explore And Correlate Definition

      View Account Template

      View Endpoint

      View Explore And Correlate Definition
5. Submit the task.

Create Correlation Rules

A Hosting Administrator or an administrator with the Configure Correlation Attributes task can create rules that are used when you explore an endpoint. The Execute Explore and Correlate task uses these rules for the correlation part of the task.

Correlation rules determine how an endpoint account attribute is mapped to a user attribute in the User Console. For example, in Access Control an attribute that is called AccountName exists. You can create a rule to map it to FullName in the User Console. If the rules cause two mappings to apply to one user attribute, the first parameter value is used.

Follow these steps:

1. Log in to the User Console.
2. Click System, Provisioning Configuration, Configure Correlation Attributes.
3. Click Add.
4. Define a correlation rule as follows:
   a. Select a global user attribute list.

      This value refers to the user attribute listed in the Provisioning Directory.

   b. Enable the Set a specific account attribute check box.
   c. Select an endpoint type.
   d. Select an account attribute that applies to the global user attribute.
   e. Optionally, complete the Substring fields.

      If the Substring from field is empty, processing begins at the start of the string. If the Substring to field is empty, processing begins at the end of the string.
5. Click OK.
6. Click Submit.

Note: Whenever you change a correlation rule, be sure to explore the endpoint even if you previously explored it.

Example of Correlation Rules

The following example provides sample settings for an Active Directory endpoint.

```
GlobalUserName
FullName=LDAP Namespace:globalFullName
FullName=ActiveDirectory:DisplayName
 CustomField01=ActiveDirectory:Telephone
```

The following actions occur for each previously uncorrelated account that is found while correlating accounts in an Active Directory container:

1. The Provisioning Server compares the first parameter value (GlobalUserName) with the Active Directory endpoint account attribute (NT_AccountID). The server attempts to find the unique global user whose name matches the NT_AccountID attribute value for that account. If a unique match is found, the Provisioning Server associates the account with the global user. If more than one match is found, the Provisioning Server performs Step 5. If no match is found, the Provisioning Server performs the next step.
2. The Provisioning Server considers the second parameter value (FullName=LDAP Namespace:globalFullName). Since this value is specific to another endpoint type, it is skipped and the Provisioning Server performs the next step.
3. The Provisioning Server considers the third parameter value (FullName=ActiveDirectory:DisplayName). Since this value is specific to Active Directory, it is used. The server attempts to find the unique global user whose FullName matches the DisplayName attribute value for that account. If a unique match is found, the Provisioning Server associates the account with the global user. If more than one match is found, the Provisioning Server performs Step 5. If no match is found, the Provisioning Server performs Step 4.
4. The Provisioning Server considers the final parameter value (CustomField01=ActiveDirectory:Telephone). Because this value is specific to Active Directory, it is used. The server attempts to find the unique global user whose Custom Field #01 attribute is equal to the Telephone attribute value for that account. The name that you gave to the custom global user attribute using global properties of the System Task is not displayed here. If a unique match is found, the Provisioning Server associates the account with the global user. If more than one match is found, the Provisioning Server performs Step 5. If no match is found, the Provisioning Server performs the next step.
5. The Provisioning Server associates the account with the [default user] object. If the [default user] object does not exist, the server creates it.

Configure Email Notification for the Endpoint

When an endpoint is created, you can have email be sent to notify users.

Follow these steps:

1. In the User Console, click System, Email, Create Email.
2. Create a copy of the following email template: CAM Create Endpoint Email.
3. Supply a unique name for the template and click the Enabled check box.
4. Click the WhenToSend tab.
5. Change the TaskCompletes event to be Create *Endpoint-Type* Endpoint Task.
6. Click the Contents tab.
7. Replace the text with whatever is required as the body of the email.
8. Click Submit.

Add the Endpoint to the Environment

You add the endpoint to the environment where you intend to manage it. Any administrator with the Create Endpoint task can perform this procedure.

Follow these steps:

1. Select Endpoints, Manage Endpoints, Create Endpoint.
2. Select an endpoint type.
3. Complete the tabs to fill in the fields.

   The required fields begin with a red circle.

   Note: Avoid using a # symbol in the endpoint name, because this character cannot be searched.
4. Click Submit.

You are now ready to create an Explore and Correlate Definition (see page 17) so that its accounts can be managed.

Create an Explore and Correlate Definition

To add users that exist in an endpoint, you create an explore and correlate definition for that endpoint. Any administrator with the Create Explore and Correlate Definition task can create the definition.

Follow these steps:

1. In an environment, click Endpoints, Explore and Correlate Definitions, Create Explore and Correlate Definition.
2. Click Okay to start a new definition.
3. Fill in Explore and Correlate name with any meaningful name.
4. Click Select Container/Endpoint/Explore Method to choose an endpoint and containers if they exist. For a large endpoint, a container search may take a while; you can use the search filter to narrow the search.
5. Click an explore method for the container. The explore and correlate process includes containers you select and its sub-containers. For a directory container, it includes all the containers in the sub-tree.

6. Click the Explore/Correlate Actions to perform:
   - **Explore directory for managed objects**—Finds objects that are stored on the endpoint and not in the provisioning directory.
   - **Correlate accounts to users**—Correlates the objects that were found in the explore function with users in the provisioning directory. Two choices of correlation exist.
     - **Use existing users**

       Use this choice for a correlation rule (see page 14) that matches each account with a previously created user.

       If the user is found, the account is correlated with that user. If multiple users are found, the account is correlated with the default user. If no user is found, this option creates the user (if all mandatory attributes are known) and correlates the account with that user; otherwise, it correlates the account with the default user.

     - **Create users as needed**

       Use this choice when correlating accounts on your primary endpoint. This option presumes that the accounts on your endpoint are named exactly the same as the users. The correlation-matching algorithm is unused with this option. Instead, each account is associated to the user with the same name. If the user does not yet exist, it is created. No accounts are associated to the default user.
   - **Update user fields**—If a mapping exists between the object fields and the user fields, the user fields are updated with data from the objects fields.

     Users are created with no optional attributes such as full name, address and telephone numbers. During the initial acquisition of an endpoint, use this option to set these user attributes using account attribute values. During subsequent explore and correlates, use this option to refresh the user attributes to apply changes made to the account attributes, perhaps by tools other than Identity Management.
7. Click Submit.

Now an administrator with the Execute Explore and Correlate (see page 19) task completes the integration of the endpoint.

Explore and Correlate the Endpoint

Hosting Administrator or another administrator with the Execute Explore and Correlate task performs this procedure. The exploration phase of the task identifies the accounts in the endpoint. The correlation phase matches the accounts with users in Identity Management or creates the accounts.

Follow these steps:

1. In an environment, click Endpoints, Execute Explore and Correlate.
2. Select Execute now to run explore and correlate immediately, or select Schedule new job to run explore and correlate at a later time or on a recurring schedule.

   Note: This operation requires the client browser to be in the same time zone as the server. For example, if the client time is 10:00 p.m. on Tuesday when the server time is 7:00 a.m, the Explore and Correlate definition will not work.
3. Click an explore and correlate definition to execute.
4. Click Submit.

   The user accounts that exist on the endpoint are created or updated in Identity Management based on the explore and correlate definition you created.
5. Verify the task succeeded as follows:
   a. Click System, View Submitted Tasks.
   b. Complete the task name field as follows: Execute Explore And Correlate
   c. Click Search.

   The results show if the task succeeded.

Note: You can abort an Explore and Correlate task when viewing the task status in View Submitted Tasks (VST). Aborting the task stops the task from processing, leaving the task in the state that it is in when you abort. Any generated notifications are sent, so that all systems are kept synchronized.

How to Set Up On-Premise Provisioning

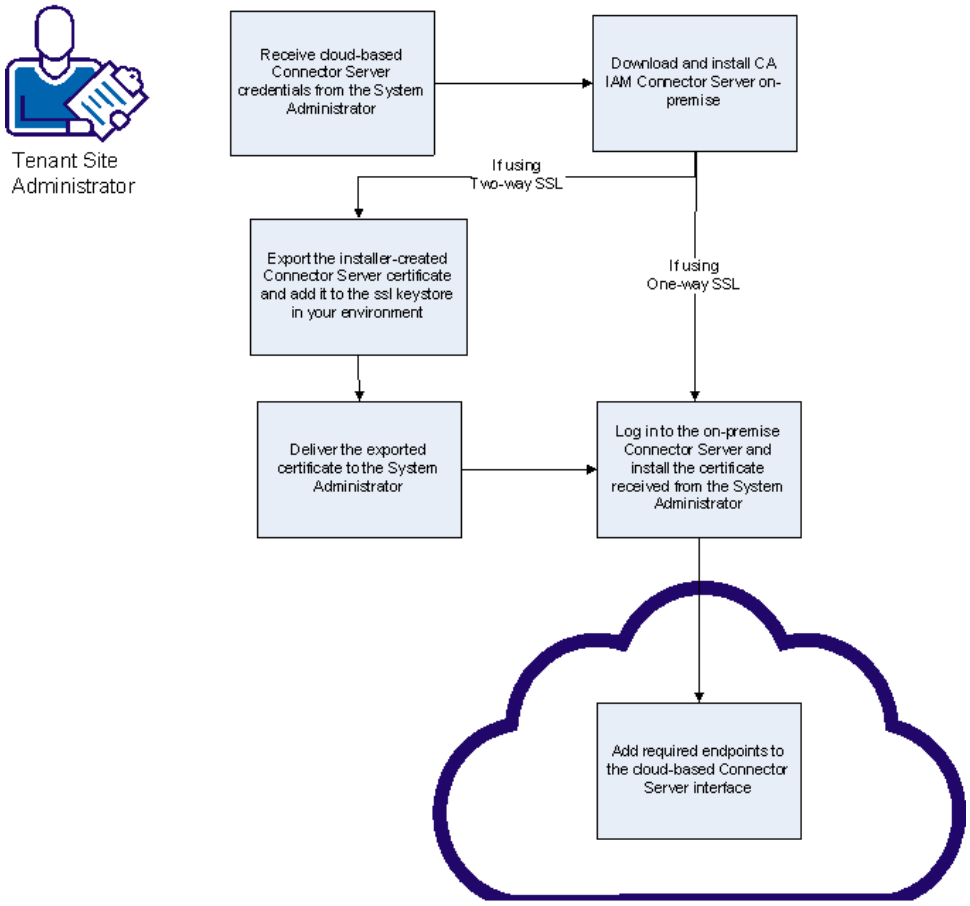
As an administrator who wishes to set up communication between cloud-based and on-premise environments and allow on-premise provisioning, follow this process:

1. Receive the username, password, the server certificate, and the URLs for the cloud-based CA IAM CS messaging interface from the CA CloudMinder System Administrator for your environment. Make a note of the time settings from the cloud-based Connector Server.
2. Download and install CA IAM CS in your on-premise environment. The installation package is available from support.ca.com.
3. Export the certificate that the connector server installer creates, and deliver it to the System Administrator if it is needed. The System Administrator tells you if this is required in your environment. If you have an existing server certificate, you can use it instead. After you install IAM Connector Server, add the certificate to the ssl keystore. The ssl keystore is a java keystore located in the jcs/conf folder of your connector server installation.

   Note: You can only add one private key to the keystore. CA IAM CS only supports one private key.
4. Install the certificate that you received from the System Administrator in your on-premise Connector Server.
5. Go to the cloud-based CA IAM CS interface and add any endpoint routes that you want.

This diagram illustrates the set-up steps:

How to Set Up On-Premise Provisioning



Install CA IAM CS

The CA IAM CS includes connectors for all of the endpoints that are supported at the time of the release.

When you install CA IAM CS, be sure to record the values you enter. The port name, password, and URL are required in other parts of the process.

Note: This procedure assumes that you do not already have a local instance of CA IAM CS installed. If you have installed it as part of an Identity Management installation, the default username is set to "admin".

Follow these steps:

1. Check the time settings for your on-premise Connector Server host. They must match the setting information that you received from the System Administrator for the two servers to connect successfully.

   Note: The cloud-based and on-premise Connector Server time zones need not match, only the settings. For example, daylight savings time must be enabled on both.

2. Download CA IAM CS from support.ca.com, and launch the installer.
3. Select the C++ connector option you want, depending on your environment.
4. Clear the "Register this installation with a Provisioning Server" checkbox if it is selected. This setting is not required for an on-premise installation.
5. On the Cloud Connector Server screen, enter the following information:
   - Server URL - The URL of the cloud-based CA IAM CS messaging interface, for example: *https://hosting.cloudminder.com/gateway/request/tenant/mytenant/*. The System Administrator provides the URL information.
   - Tenant Name
   - Tenant Host ID - Optional identification for an environment with multiple on-premise server installations.
   - Username - The user name that the System Administrator created for this tenant.
   - Password - The password that the System Administrator created for this tenant.

   Note: To connect to a cloud-based Connector Server, enter details in this step. The details are required for the installer to create a key pair and self-signed certificate. If for some reason you cannot enter details on initial installation, rerun the installer and add details before completing the connection.
6. Enter the admin password on the Connector Server Configuration screen, and accept the default LDAP port values.

Note: If you install multiple connector servers, be sure to set the same password for each. This practice avoids a password synch issue.

7. On the Port Configuration screen, accept the default values.
8. Enter HTTP Proxy credentials if your environment uses an HTTP proxy.
9. Complete the wizard. You can install multiple connector servers in your environment, depending on your needs.

Export a Certificate

The CA IAM CS installer creates a self-signed certificate. If you are a Site Administrator preparing for on-premise provisioning, you can locate and export the certificate file to deliver to the CA CloudMinder System Administrator.

Follow these steps:

1. Log in to the on-premise CA IAM CS.
2. Select the Certificates tab, and locate the new certificate. The certificate is a Private Key type, "tenant_name". You can sort the Type or Name columns to help locate the certificate.
3. Select the new certificate, click Download, and save the file in a location of your choice.
4. If you are using two-way SSL certification in your environment, send the certificate file to the System Administrator using a trusted mechanism.

Configure the On-Premise Connector Server

To set up on-premise provisioning, add the certificate that you received from the CA CloudMinder System Administrator to your on-premise connector server.

Follow these steps:

1. Log in to CA IAM CS in your CA CloudMinder environment.
2. Click the Certificates tab in the Connector Server Management pane.

   The Add Certificate dialog appears.
3. Browse to the location where you saved the certificate file, select it, and click Add.
4. Enter the certificate alias, and Click OK.

   The certificate appears in the certificate list.
5. Select the Servers tab. Select the cloud connector server entry, and click Modify.

   The Modify Connector Server dialog appears.
6. Enter or add to the credentials for the target connector server, including the tenant name, and click OK.

   You can test the connection to make sure that the components are communicating properly.

Configure the Cloud-Based Connector Server

To complete the set-up process for on-premise provisioning, you add endpoint routes. You can configure the default on-premise connector server or any other on-premise connector server in your environment. You can also add a connector server then add routes to that connector server.

Follow these steps:

1. Log in to the CA CloudMinder user console and navigate to Task>System>Manage Connector Server.
2. Click Add to add a connector server.
   a. Supply any name for the connector server.
   b. Click OK.
   c. After a minute, click Status to display the new connector server.
3. Select the connector server entry to which you want to add a route.
4. Right-click the connector entry and select Add Routes from the popup menu.
5. Check the route or routes that you want to add, and click OK.

   You can add routes to more than one connector server. If you have added an Active Directory route to one connector server, it is not available to add to other connector servers.

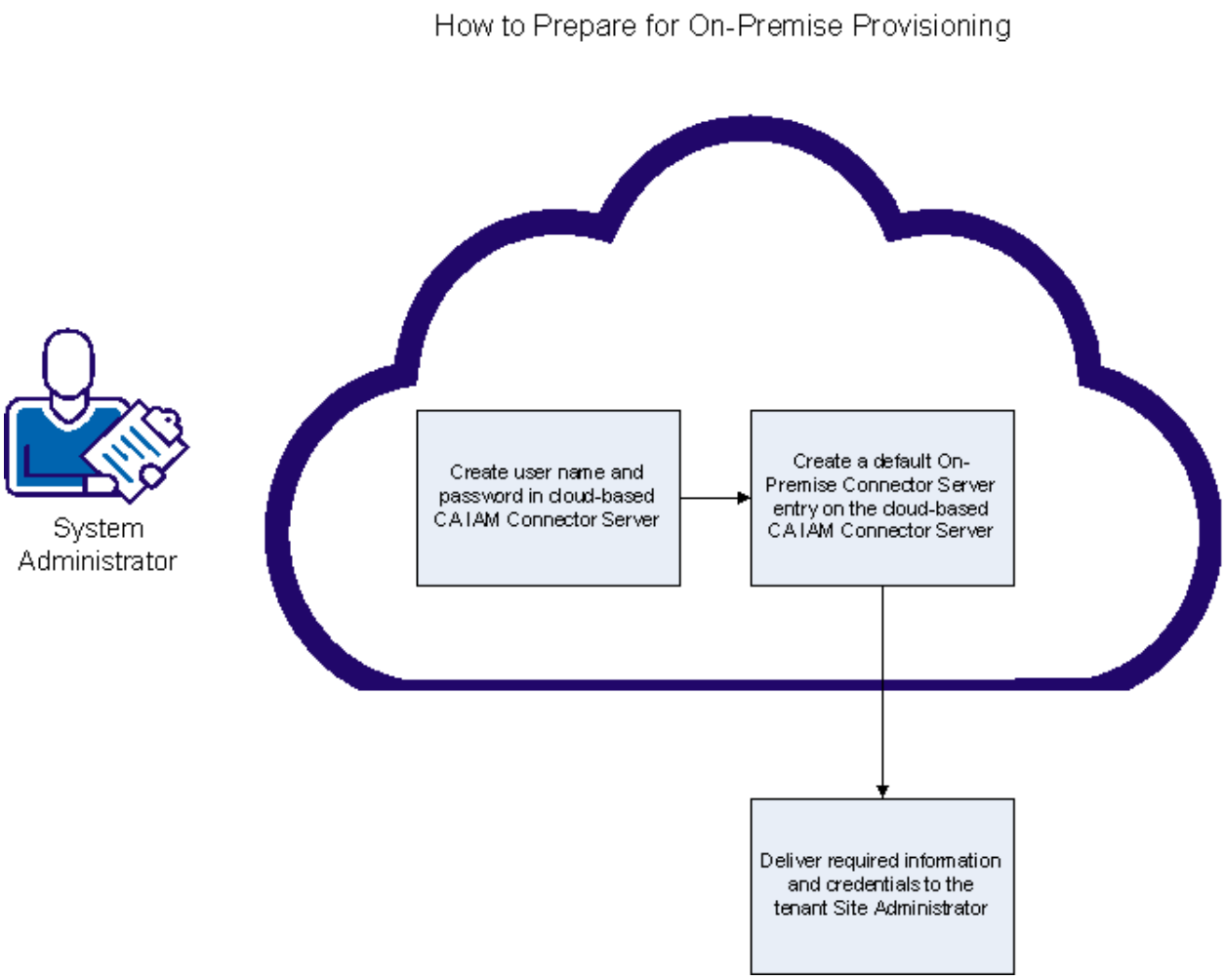
How to Prepare for On-Premise Provisioning

As a CA CloudMinder System Administrator, you can prepare the tenant environment for on-premise provisioning. Follow this process:

1. Ensure that CA IAM CS is available for download by the tenant Site Administrator.
2. Log in to the cloud-based CA IAM CS, and create a username and password for the tenant.
3. Create a default on-premise server entry for the tenant.
4. Deliver the following items to the Site Administrator:
   - Username and password
   - The cloud CA IAM CS certificate

     Note: If you plan to access the cloud-based connector server using a gateway such as an http reverse proxy, provide the server certificate of the gateway *instead* of the CA IAM CS certificate.
   - The URL of the cloud-based CA IAM CS messaging interface and the URL of the cloud-based CA IAM CS management interface
   - Time settings for the cloud-based Connector Server, for example whether daylight savings time is enabled on the host computer.

This diagram illustrates the preparation steps:



Create Tenant Credentials

You can create a username and password for a tenant to access CA IAM CS.

Follow these steps:

1. Log in to the cloud-based CA IAM CS using the admin credentials you specified during the connector server installation.

   Note: This admin user is associated with the Connector Server itself, and not with any specific tenant.

2. Select the Users tab, and click Add.
3. Enter a username, email and password in the Add User dialog.
4. Click Add to open the tenant name dialog, enter the name of the tenant this user is associated with, and click OK. You can add multiple tenant names by repeating this step.
5. Click OK in the Add User dialog. Record the name and credentials for delivery to the tenant Site Administrator.

Create a Default On-Premise Server Entry

You can create a default entry for the on-premise CA IAM CS that the tenant Site Administrator installs. The Site Administrator can add additional entries later if they have more than one connector server installed on-premise.

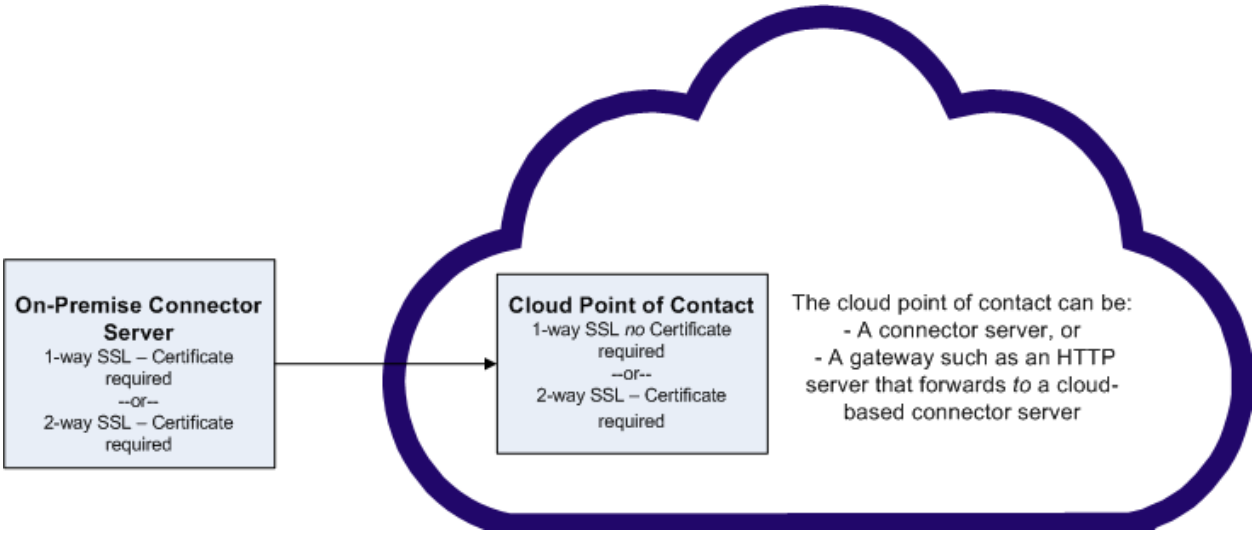
Follow these steps:

1. Log in to the cloud-based CA IAM CS, and select the Servers tab.
2. Click Add.
3. Ensure that "On Premise" is selected in the Add Server dialog.
4. Enter the tenant name.
5. Leave the default domain name, im.
6. (Optional) Enter a tenant Host ID. This is only required if the Site Administrator plans to install multiple on-premise connector servers.
7. Click OK.

Certificate Deployment

You use one or more certificates to allow communication between the on-premise and cloud installations of CA IAM CS. The communication method that you use controls where you must install certificates.

The two cases for certificate deployment are illustrated in the following diagram:



- 1-way SSL - Deploy the server certificate from the cloud point of contact in the on-premise connector server.
- 2-way SSL - Deploy the cloud point of contact certificate on the on-premise connector server. Also deploy the server certificate of the on-premise connector server on the cloud point of contact.

Depending on your environment, the cloud point of contact could be either:

- A CA IAM CS. In this case there, is a direct connection between the on-premise and cloud connector servers. This means that the SSL connection and certificate exchange is between the cloud connector server and the on-premise connector server.
- An HTTP gateway such as an Apache HTTP server, or reverse proxy server. In this case, the on-premise connector server connects directly to the HTTP gateway, which forwards requests to a cloud-based connector server. This means that the SSL connection and certificate exchange is between the HTTP gateway and the on-premise connector server.

For two way-SSL deployments, once the tenant Site Administrator creates a certificate, you can add it to the cloud point of contact. The Site Administrator provides the certificate file to you using a secure mechanism of your choice, secure file transfer, or CD for example.

More information:

Install a Certificate (see page 30)

Install a Certificate

You can install a certificate on a connector server. For more information about which servers to deploy certificates on, see Certificate Deployment.

Follow these steps:

1. Log in to the cloud-based, or the on-premise connector server, as needed.
2. Click the Certificates tab in the Connector Server Management pane.

   The Upload Certificate dialog appears.
3. Select Certificate if the target is a standalone certificate file, or Key Store, if it is saved in a key store.
4. Browse to the tenant certificate, select it, and click Add.
5. Enter the required alias. If you selected Key Store, enter the required key store password.
6. Click OK.

More information:

Certificate Deployment (see page 29)

Deliver Tenant Information

To allow the tenant Site Administrator to set up on-premise provisioning, deliver the following information:

1. Credentials, including username, password, and tenant name. Also enter the domain name, if you are using a different name from the default.
2. The URL of the cloud-based CA IAM CS, which uses one of the following formats:
   - https://*cloudcs_hostname*:20443 - for direct communication.
   - https://*gateway_hostname/redirect_rulename* - for environments using a gateway redirect.
3. The URL of the cloud-based messaging server interface - It uses one of the following formats:
   - https://*cloudcs_hostname*:22002- for direct communication.
   - https://*gateway_hostname/redirect_rulename*

   Note: Replace the items in italics with the appropriate values from your environment. The port numbers shown here are the default values. If you have changed the ports, use the appropriate numbers. *Redirect_rulename* is the name of the redirect rule.
4. The CA IAM CS cloud server certificate. If you plan to provide access to the cloud-based connector server using a gateway, such as an http reverse proxy, do not send the cloud server certificate. Instead, provide the server certificate of the gateway.
5. Time settings for the cloud-based Connector Server. The time settings for the cloud-based and on-premise servers must match for the servers to be able to connect. The time zones need not match, but settings must, such as whether daylight savings time is enabled on the cloud Connector Server host.

Set Up Identity Management Provisioning with Active Directory

You can use Active Directory Server (ADS) to synchronize attribute data to supported endpoints. You do this by configuring CA IAM CS to propagate local changes in Active Directory to a cloud-based identity store using a connector.

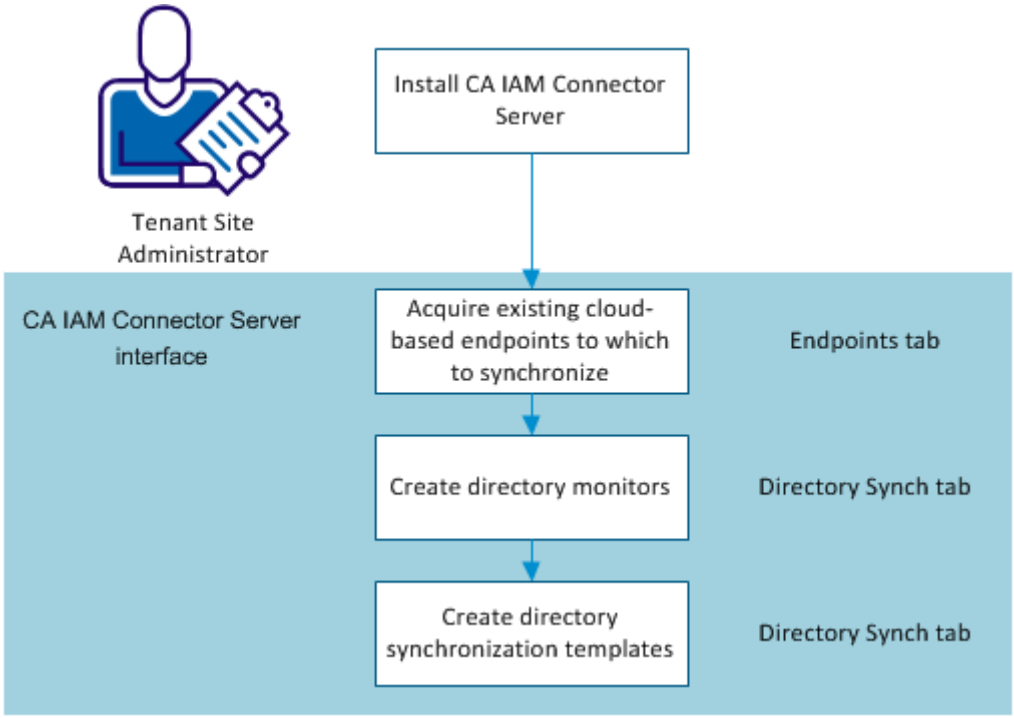
For example, assume that you have a SalesForce installation in the cloud. You could create an ADS group named "SalesForce" and then configure the CA IAM CS to monitor that group. CA IAM CS synchronizes any changes to the SalesForce environment in the cloud.

If you add a user to the ADS Salesforce group, CA IAM CS uses the SalesForce connector to trigger a "Create User" action in the SalesForce environment proper.

To set up directory synchronization, follow this process:

1. Install CA IAM CS in your environment.
2. Acquire the endpoints that you want to synchronize with. Consult the appropriate connector configuration documentation. You must acquire endpoints in order to create templates in step 4.
3. Create one or more directory monitors. Monitors capture changes that you make in your local Active Directory, and report them for the synchronization.
4. Create one or more synchronization templates. Templates control settings for the directory synchronization.

Figure 1: Flowchart showing the steps to set up directory sychronization



Install CA IAM CS

Install CA IAM CS to set up directory synchronization to endpoints such as SalesForce

Follow these steps:

1. Download CA IAM CS from support.ca.com, and launch the installer.
2. The C++ connector server is not required for directory synchronization.
3. Clear the "Register this installation with a Provisioning Server" checkbox if it is selected. This setting is not required.
4. You need not enter any information about the Cloud Connector Server screen for the purpose of this configuration.
5. Enter the admin password on the Connector Server Configuration screen, and accept the default LDAP port values.
6. On the Port Configuration screen, accept the default values.
7. Complete the wizard.

Create a Directory Monitor

Create a directory monitor to find and report changes in your on-premise Active Directory installation. Monitors receive change notifications. Directory synchronization templates then control how the changes are processed.

Follow these steps:

1. Select the Directory Sync tab, and click Add in the Monitor area.

   The Add Monitor dialog appears. Both the ADS domain and forest you want to monitor must be Windows 2003 or later.

   Note: if you are using ldaps, first import the ADS certificate in the Certificates tab. See *Directory Synchronization with Active Directory* for more information.

2. Enter the URL of the Active Directory installation you want to monitor. Type it, or modify the default URL template with the appropriate hostname and port number.
3. Enter User Distinguished Name information to grant access to ADS for synchronization. The user DN you enter must correspond to a valid user object in the Active Directory instance you want to monitor.
4. Enter a password, if necessary for your active directory installation.
5. Click Browse to connect to the ADS and locate a valid Search Base.
6. You can test the LDAP connection if you have entered a password.
7. Click OK.

You can also set connection pool details, such as how many connections can be active at any time.

Create a Directory Synch Template

Synchronization templates control how local changes are propagated to your endpoints, and how they are formatted. You can create synchronization templates for each of the endpoint types you want to control from your ADS installation. You can also create multiple templates for a single endpoint to subdivide the synchronization data, by business unit, for example.

Add one or more templates to each directory monitor in your environment. Add directory monitors before you can add synchronization templates.

Follow these steps:

1. Log in to CA IAM CS, and select the Endpoints tab to see the available endpoints that you can synchronize with.
2. Select the Directory Sync tab, then click the monitor entry where you want to add a synchronization template, and click Add in the Template area.

   The Add Template dialog appears.
3. Select the template type that you want from the drop-down menu, and then select an available endpoint name.
4. Select the User Store tab to set User Store details:
   a. Click Add in the Trigger Groups area.
   b. Enter a filter value if you want to refine the search for available groups. You can also accept the default in the Add Trigger group dialog.
   c. Click Search.

      A list of available Active Directory groups appears.
   d. Select the group or groups you want using the shuttle control, and click OK.
5. Select the Attributes tab to configure how the template maps Active Directory source information to the target endpoint:

   A list of default attributes appears. Attributes that are required for your template type are displayed in bold type.
   a. Set required attribute mappings by selecting available mapping targets from the Maps To pull-down menu. You can also type a literal string.
   b. Set mappings for other available attributes as desired. Select a policy setting (WEAK or STRONG) for each mapping you add.

      For single-value attributes, you need only be sure that the policy is not NONE. For multivalue attributes, Strong replaces any existing attribute value in the endpoint, and weak adds the new attribute value to any existing endpoint values.
   c. If the standard mapping table does not meet your needs, use the advanced editor. Click Advanced to display the editor. The advanced editor allows you to:

- Use JavaScript evaluated attribute values.
- Pick object references for association values.
- Set alternate attribute mappings or default values that apply when the primary mapping cannot be resolved.

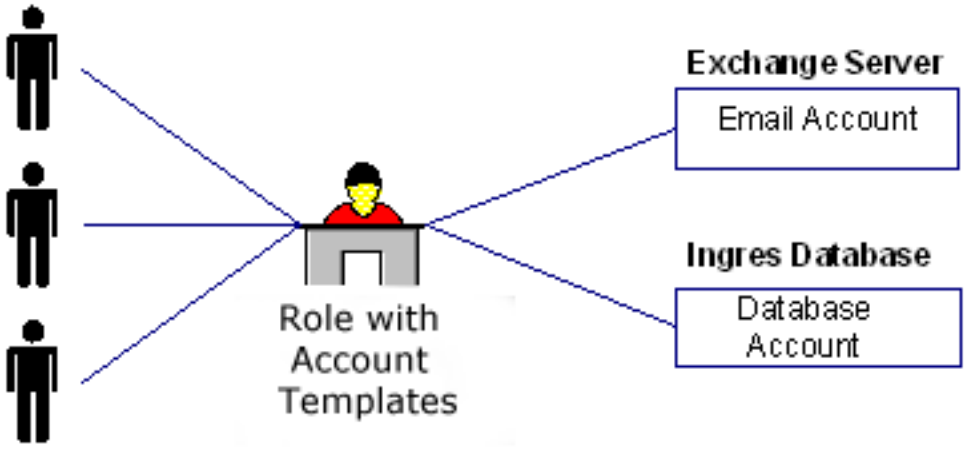
6. Click OK.

Creating Roles to Assign Accounts

In most organizations, administrators spend significant time providing users with login accounts for different systems and applications. To simplify this repetitive activity, you can create provisioning roles, which are roles that contain account templates. The templates define the attributes that exist in one type of account. For example, an account template for an Exchange account defines attributes such as the size of the mailbox. Account templates also define how user attributes are mapped to accounts.

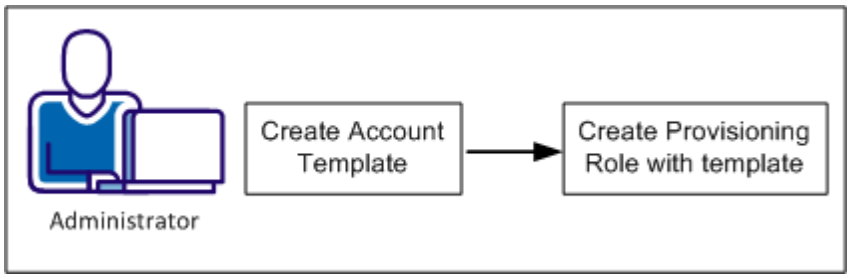
Consider an example where every employee at Forward, Inc needs access to a database and email. An administrator wants to avoid creating a database account and an email account for each employee one at a time. Therefore, the administrator creates a provisioning role for that company. The role contains an account template for a Microsoft Exchange server, to provide email accounts, and a template for an Oracle database. In this example, the Exchange server and the Oracle database are named endpoints, which are the system or application where the accounts exist.

Note: Forward, Inc. is a fictitious company name which is used strictly for instructional purposes only and is not meant to reference an existing company.



After the roles are created, business administrators, such as managers or support personnel, can assign those roles to users to give them accounts in endpoints. After users receive the role, they can log in to the endpoint.

Creating a provisioning role that includes an account template is a two-step process as follows:



The following sections explain how to create a role that can be used to assign accounts:

1. Create an Account Template (see page 37)
2. Create a Provisioning Role (see page 40)

Create an Account Template

A default account template exists for each endpoint type. In a provisioning role, you can use the default account template. However, you can create your own account templates for any endpoint that you have configured.

Follow these steps:

1. Log in to the User Console and select Endpoints, Manage Account Templates, Create Account Template.

   A screen appears with a list of endpoint types.

2. Select an endpoint type for the template.
3. Complete the Account Template tab.
   a. Provide an account template name.
   b. Select Use Strong Synchronization for the maximum correlation of the account template and endpoint account.
4. Complete the Endpoints tab.
   a. Select an endpoint.
   b. Define Endpoint Name as the system name of the endpoint or localhost if that applies.
5. Complete the Account tab.
   a. Modify the rule strings (see page 38) in percent signs if necessary. The rules strings define the format of Login fields for the account.
   b. Enter a %AC% rule string in the Account Name field. You enter this string because account names must be unique.

6. Complete the fields in the other tabs or use the default values.

   Each endpoint type has a different set of tabs. Click Help for field definitions.

7. Click Submit.

CA CloudMinder creates the account template and makes it available for use in provisioning roles.

Rule Strings in Account Templates

When you create an account template, you use rules strings to define the format of many account attributes. Rule strings are variables for the actual value. Rules strings are useful when you want to generate attributes that change from one account to another. When rules are evaluated, Identity Management replaces the rule strings entered in the account templates with data specified in the user object.

Note: Rule evaluation is not performed on accounts created during an exploration or on accounts created without provisioning roles.

The following table lists the rule strings in Identity Management:

Rule String	Description
%AC%	Account name
%D%	Current date in the format *dd/mm/yyyy* (the date is a computed value that does not involve the global user information*).* This rule string is equivalent to one of the following: %$$DATE()% %$$DATE%
%EXCHAB%	Mailbox hide from exchange address book
%EXCHS%	Mailbox home server name
%EXCMS%	Mailbox store name
%GENUID%	Numeric UNIX/POSIX user identifier. This rule variable is the same as %UID% as long as the global user UID value is set. However, if the global user has no assigned UID value, and UID-generation is enabled (Global Properties on System Task), several actions occur. The next available UID value is allocated, assigned to the global user, and used as the value of this rule variable.
%P%	Password

Rule String	Description
%U%	Global user name
%UA%	Full address (generated from street, city, state, and postal code)
%UB%	Building
%UC%	City
%UCOMP%	Company name
%UCOUNTRY%	Country
%UCU*xx*% or %UCU*xxx*%	Custom field (*xx* or *xxx* represents the two-digit or three-digit field ID as specified on the Custom User Fields tab in the System Task frame)
%UD%	Description
%UDEPT%	Department
%UE%	Email address
%UEP%	Primary email address
%UES%	Secondary email addresses
%UF%	First name
%UFAX%	Facsimile number
%UHP%	Home page
%UI%	Initials
%UID%	Numeric UNIX/POSIX User Identifier
%UL%	Last name
%ULOC%	Location
%UMI%	Middle initial
%UMN%	Middle name
%UMP%	Mobile telephone number
%UN%	Full name
%UO%	Office name
%UP%	Telephone number
%UPAGE%	Pager number
%UPC%	Postal code, ZIP Code
%UPE%	Telephone number extension

Rule String	Description
%US%	State
%USA%	Street address
%UT%	Job title
%XD%	Generates the current timestamp in XML dateTimeValue format, a fixed-length string format. In a dateValue or timeValue attribute, you can write an (:offset,length) substring expression to extract the date or time parts of the dateTimeValue. For example, %XD:1,10% yields YYYY-MM-DD; and %XD:12,8% yields HH:MM:SS.

Create a Provisioning Role

After you create the account template, you decide about the role requirements, as follows:

- The accounts that apply to the role
- Who can assign this role
- Who can modify this role

After you decide about the role requirements, you are ready to create a provisioning role.

Follow these steps:

1. Log in to the User Console and click Roles and Tasks, Provisioning Roles, Create Provisioning Role.
2. Complete the Profile tab.

   Only the Name field is required unless you are using a customized version of Create Provisioning Role.
3. Complete the Account Templates tab.
   a. Click an endpoint type, such as SAP.
   b. Click an account template.

      The templates that you can click are based on the endpoint type you selected.
   c. Add more account templates if needed for different endpoint types.
4. Complete the Administrators tab and Owners tab.

   Add admin rules that control who manages members and administrators of this role.

   Add owner rules that control who can modify this role.

5. Click Submit.

   A message appears to indicate the status of the Create Provisioning Role task.

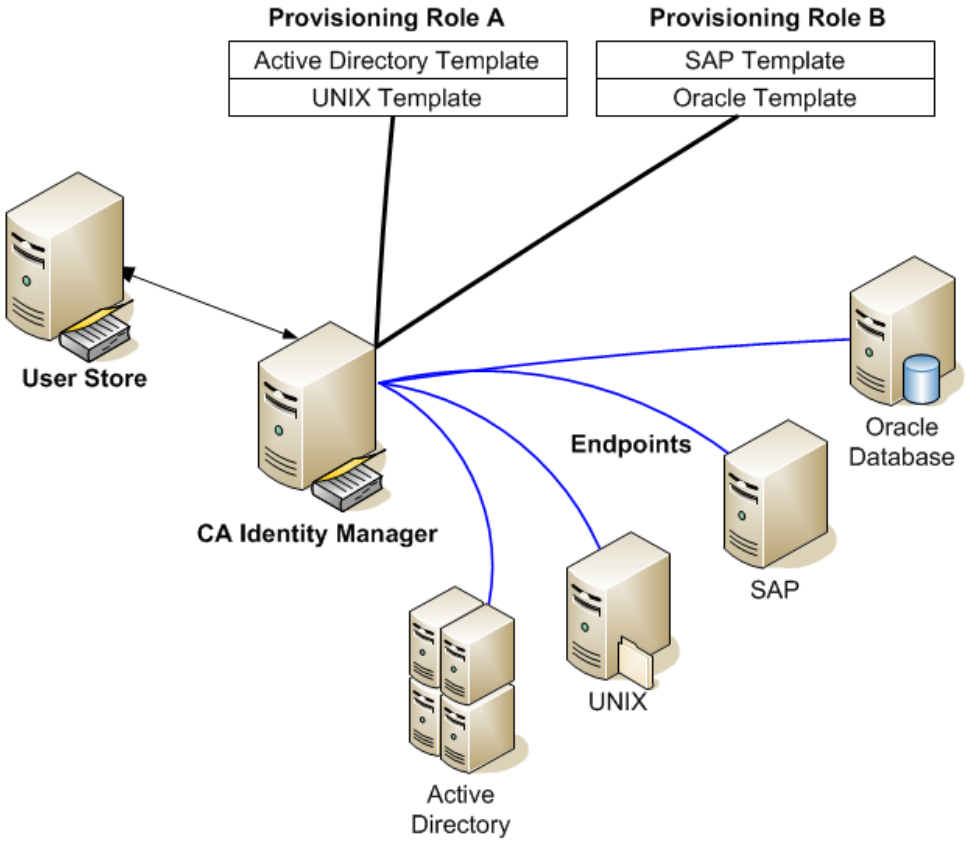
6. To verify that the role was created, click Roles and Tasks, Provisioning Roles, View Provisioning Role.

You have now successfully created a provisioning role. The role can now be assigned to users, so that they can access the accounts that they need.

Synchronize Users, Accounts, and Roles

The integration of multiple endpoints and accounts into a single user management system can result in a loss of synchronization. The provisioning roles or account templates that are assigned to a user can differ from the actual accounts that exist for that user.

For example, consider a situation with two provisioning roles, one with Active Directory and UNIX account templates and another role with SAP and Oracle templates. The user john_smith has Provisioning Role A, which contains Active Directory and UNIX account templates, but that user only has an Active Directory account. Possibly the UNIX account template was added to the role after it was assigned to the user. Therefore, the administrator synchronizes the user with the current role definition.



The following situations are other reasons why users lose synchronization with provisioning roles or account templates:

- Earlier attempts to create the necessary accounts failed due to hardware or software problems in your network, causing missing accounts.
- Provisioning roles and account templates change, and this creates extra or missing accounts.

- Accounts were assigned to account templates after they were created, so accounts exist, but they are not synchronized with their account templates.
- The creation of a new account is delayed because the account was specified to be created later.
- A new endpoint was acquired. During exploration and correlation, the Provisioning Server did not assign provisioning roles to the users automatically. You update the role to indicate the users who require accounts on the endpoint. Any account that was correlated to a user is listed as an extra account when the user is synchronized.
- An existing account was assigned to a user by copying the account to the user.
- An account was created for a user other than by assigning the user to a role. For example, you copied a user to an account template that is not in a provisioning role for that user. The account is listed as an extra account or as an account with an extra account template. If you copy the user to an endpoint to create an account using the default account template, that account could be an extra account.

The following sections explain how to perform the three types of synchronization:

1. Synchronize users with roles (see page 44).
2. Synchronize user with account templates (see page 44).
3. Synchronize endpoint account with account templates (see page 46).

Synchronize Users with Roles

This task creates, updates, or deletes accounts so they comply with the provisioning roles assigned to a user. For example, administrators use native tools on an endpoint to add or delete accounts, but you have not reexplored that endpoint to update the provisioning directory. Therefore, users have extra or missing accounts. This task also ensures that each account belongs to the correct account templates.

Follow these steps:

1. Log in to the User Console.
2. Select Tasks, Users, Synchronization, Check Role Synchronization.
3. Select a user.

   A screen appears showing the expected accounts, extra accounts, and missing accounts.
4. Click Synchronize to make the accounts match the template in this role.
   a. You can select a checkbox to create the account on the endpoint. If more than one account template for the user prescribes the same account, the account is created by merging all relevant account templates.

      This account is assigned to those account templates, which are currently not synchronized with the account.
   b. You can select a checkbox to delete extra accounts. However, users can have legitimate reasons for having these accounts. If that is the case, leave this option unchecked.

      On certain endpoints, the account deletion function is disabled; therefore, the account is not deleted.

Synchronize User with Account Templates

This task synchronizes the attributes for endpoint accounts with the associated account templates for a user. However, full synchronization depends on these factors:

- Full synchronization of the account occurs in two situations. An account template uses strong synchronization (see page 47) or two or more account templates were added to an account.
- If an account template uses weak synchronization (see page 47), this task starts an account synchronization involving only this template. If the account was previously out of account synchronization with other account templates before this update, it could still be out of account synchronization afterwards.

Follow these steps:

1. Log in to the User Console.
2. Select Tasks, Users, Synchronization, Check Account Template Synchronization.
3. Select a user.

   A screen appears showing the expected accounts, extra accounts, and missing accounts.
4. Click Synchronize to make the accounts match the template.
   a. You can select a checkbox to create the account on the endpoint. If more than one account template for the user prescribes the same account, the account is created by merging relevant account templates.

      This account is assigned to the account templates that are not synchronized with the account. Account synchronization is not necessary on newly created accounts.
   b. You can select a checkbox to delete extra accounts. However, users can have legitimate reasons for having these accounts. If that is the case, leave this option unchecked.

      On certain endpoints, the account deletion function is disabled; therefore, the account is not deleted.

Attributes Only for New Accounts

In an account template, certain attributes are only applied when creating the account. For example, the Password attribute is a rule expression that defines the password for new accounts. This rule expression never updates the password of an account. Changes to the password rule expression only affect accounts that are created after the rule expression was set.

Similarly, a template rule expression for a read-only account attribute affects only accounts that are created after the rule expression was set. Changing it has no effect on existing accounts.

Synchronize Endpoint Accounts with Account Templates

This task synchronizes an endpoint account after modification of an associated account template. For example, perhaps an Active Directory account has no groups, but the associated account template is defined to include groups.

Follow these steps:

1. Log in to the User Console.
2. Select Tasks, Endpoints, Manage Endpoints, Check Endpoint Account Synchronization.
3. Select an endpoint.

   A screen appears showing accounts on that endpoint, associated account templates, and which attributes are not synchronized.
4. Click Synchronize to make the attributes for those accounts match what is defined in the account template.

   Changes that you make to account templates affect existing accounts as follows:

   - If you change the value of a capability attribute, the corresponding account attribute is updated to be synchronized with the account template attribute value. See the description of weak and strong synchronization.
   - Certain account attributes are designated by the connector as not being updated on account template changes. Examples include certain attributes that the endpoint type allows to be set only during account creation, and the Password attribute.

Which Attributes are Updated

When you change capability attributes in an account template, the corresponding attribute on the accounts change. This change has an impact on the attributes for the account. The impact is based on the following factors:

- Whether the account template is defined to use weak or strong synchronization.
- Whether the account belongs to multiple account templates.

Weak Synchronization

Weak synchronization ensures that users have the minimum capability attributes for their accounts. Weak synchronization is the default in most endpoint types. If you update a template that uses weak synchronization, Identity Management updates capability attributes as follows:

- If a number field is updated in an account template and the new number is greater than the number in the account, Identity Management changes the value in the account to match the new number.
- If a check box was not selected in an account template and you subsequently select it, Identity Management updates the check box on any account where the check box is not selected.
- If a list is changed in an account template, Identity Management updates all accounts to include any value from the new list that was not included in the account's list of values.

If an account belongs to other account templates (whether those templates use weak or strong synchronization), Identity Management consults only the template that is changing. This action is more efficient than checking every account template. Because weak synchronization only adds capabilities to accounts, it generally is not necessary to consult those other account templates.

Note: When propagating from a weak synchronization account template, changes that would remove or lower capabilities could leave some accounts unsynchronized. Remember that with weak synchronization, capabilities are never removed or lowered. Without consulting other templates for an account, the propagation does not consider if weak synchronization is sufficient.

In this situation, use Synchronize Users with Account Templates to synchronize the account with its account templates.

Strong Synchronization

Strong synchronization ensures that accounts have the exact account attributes that are specified in the account template.

For example, suppose that you add a group to an existing UNIX account template. Originally, the account template made accounts members of the Staff group. Now, you want to make the accounts members of both the Staff and System groups. All accounts that are associated with the account template are considered synchronized when each account is a member of the Staff and System groups (and no other groups). Any account not in the Staff group is added to both groups.

Some other factors to consider include the following situations:

- If the account template uses strong synchronization, any account belonging to groups, other than Staff and System, are removed from those extra groups.
- If the account template uses weak synchronization, the accounts are added to the Staff and System groups. Any account that has additional groups that are defined to it remains a member of these groups.

Note: Synchronize accounts with their templates regularly to ensure that the accounts stay synchronized with their account templates.

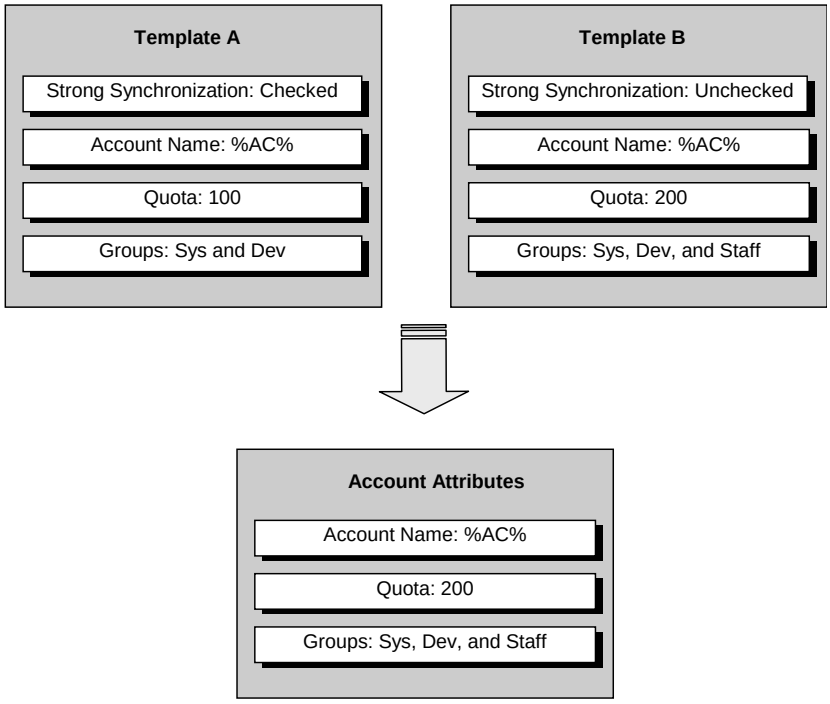
Accounts with Multiple Templates

Synchronization also depends on whether the account belongs to more than one account template. If an account has only one account template and that template uses strong synchronization, each attribute is updated to exactly match what the account template attribute value evaluates to. The result is the same as if the attribute were an initial attribute.

An account may belong to multiple Account Templates, as would be the case if a user belonged to multiple provisioning roles each of which prescribed some level of access on the same managed endpoint. When this happens, Identity Management combines those account templates into one effective account template that prescribes the superset of the capabilities from the individual account templates. This account template is itself considered to use weak synchronization if all its individual account templates are weak or strong synchronization if any of the individual account templates is strong.

Note: Often you use only weak synchronization or only strong synchronization for the account templates controlling one account, depending on whether your company's roles completely define the accesses your users need. If your users do not fit into clear roles and you need the flexibility to grant additional capabilities to your user's accounts, use weak synchronization. If you can define roles to exactly specify the accesses your users need, use strong synchronization.

The following example demonstrates how multiple account templates are combined into a single effective account template. In this example, one account template is marked for weak synchronization and the other for strong synchronization. Therefore, the effective account template created by combining the two account templates is treated as a strong synchronization account template. The integer Quota attribute takes on the larger value from the two account templates, and the multivalued Groups attribute takes on the union of values from the two polices.



Reverse Synchronization with Endpoint Accounts

Although it is the responsibility of Identity Management to create, delete and modify accounts, it is impossible to prevent an endpoint system user from performing these operations on their own. This situation can occur due to emergency reasons, or malicious reasons, such as a hacker. Reverse Synchronization ensures control of the accounts a user has on each endpoint by identifying discrepancies between Identity Management accounts and accounts on the endpoints.

For example, if an account was created in the Active Directory domain using an external tool, Identity Management must be aware of this potential security issue. In addition, bypassing Identity Management causes a lack of approval processes, and audit reports.

Two types of discrepancies between Identity Management and managed endpoints are as follows:

- A new account detected
- A change within an existing account

You can treat both cases by defining policies to handle the change. Then, using Explore and Correlate to update Identity Management, you trigger the execution of policies.

How Reverse Synchronization Works

Reverse synchronization with endpoint accounts occurs as follows:

1. An administrator or a malicious user creates or modifies an account on an endpoint.
2. When Explore and Correlate runs on that endpoint, the new or modified account is detected.
3. The Provisioning Server sends a notification to the Identity Management server.
4. The Identity Management server searches for a reverse synchronization policy that matches the change on the endpoint.
5. If a matching policy is found, it executes. If more than one policy applies to this account and those policies have the same scope, the highest priority policy runs.
6. Depending on the policy, one of the following actions occurs:
   - For a new account, the policy accepts, deletes, or suspends the account or sends it for workflow approval.
   - For a modified account, the policy accepts the value, reverts it to the last known value, or sends it for workflow approval.
7. If workflow is selected, a new event for the workflow is generated and the approvers are set. Then, one of the following actions occurs:
   - For a new account, the approver can accept, delete, or suspend the account or assign it to a user.
   - For a modified account, the workflow process is the same as if the value was changed in the User Console, except that rejected values are reverted at the endpoint.

Map Endpoint Attributes

To use reverse synchronization on an attribute in an endpoint account, you first map it to an attribute visible in the User Console. Some attributes, such as account name and password, are mapped by default. Other attributes are not mapped. For example, the Active Directory attribute group membership is not mapped. For some endpoint types, no attributes are mapped.

To check if the attribute can be mapped

1. In the User Console, click Endpoints, or Tasks, Endpoints.
2. Click Reverse Modify, Create Reverse Sync Modified Account Policy.
3. Choose to create a new policy or a copy of a policy.
4. Click Endpoint Type and choose an endpoint, such as Active Directory.
5. Click Attribute Name to display a list of attributes that can be mapped.
6. Click Cancel.

   You cancel the policy because you are only using it now to check which attributes can be mapped.

Important! You can manage certain attributes only by native tools on the endpoint. So if an endpoint user modifies this type of attribute, the reverse event fails when the reverse synchronization policy is triggered. However, changes to other attributes in that reverse event are not reversed. Therefore, avoid mapping attributes that can only be managed on the endpoint.

To map endpoint attributes for reverse synchronization

1. Click Endpoints, Modify Endpoint.
2. Search for and select an endpoint that requires reverse synchronization.
3. Click the Attribute Mapping tab.
4. Select Use Custom Settings.
5. Click Add to add a new custom attribute.
6. Select an available custom attribute. For example, use CustomField 10 if it is not used in your environment.
7. Map the custom attribute to the account attribute name that you want to manage.
8. Repeat Steps 5 to 7 to add mappings between all account attributes required and the custom attribute selected.

   You can use the same custom attribute (CustomField 10 in our example) for all attributes you want to manage.
9. Click Submit.

To create baseline values for this endpoint

Once all values for an endpoint are mapped, you explore the endpoint. For this operation, you disable inbound notification and enable it after the explore completes. Disabling notification eliminates notifications that are unnecessary. Otherwise, every account that has values on the new attributes would generate a notification during the explore operation.

1. In Provisioning Manager, disable inbound notification as follows:
   a. Click System, Domain configuration, Identity Management Server, Enable Notification.
   b. Select No.
   c. Restart the Provisioning Server to make sure the change takes effect.
2. In the User Console, click Endpoints, Execute Explore and Correlate.

   Choose an explore and correlate definition that has correlation deselected.

   This action repopulates the user store attributes with the new endpoint attribute data. This task may take a while if the endpoint is large.
3. Reenable inbound notification in Provisioning Manager.
4. Restart the Provisioning Server.

At the next explore and correlate operation for that endpoint, modify account notifications are generated. Notifications are generated if a change occurred for an attribute that is mapped to a global user attribute and a policy applies to that attribute.

Policies for Reverse Synchronization

When an account is created or modified on an endpoint, reverse synchronization policies can take appropriate actions in response. For example, a user creates some Active Directory accounts in several OUs in the corporate domain. Also, the user modifies some Microsoft Exchange accounts. You can detect the new and changed accounts and provide appropriate actions as a response using reverse synchronization account policies.

You can do the following using reverse synchronization:

- Configure a policy to accept the new account, reject it, or send it for workflow approval.
- Configure a policy to accept a change to an attribute, revert it to the original attribute, or send it for workflow approval.
- When an account is sent for workflow approval, the approver can perform one of the following actions:
  - Reject it (delete/suspend it from the endpoint or change the value to match the Identity Management user store value)
  - Accept it and update the Identity Management user store to match the account
  - Assign it to a user in User Console (in the case of account creation)

Create a Policy for New Accounts

If you want to define a process for when a new account is detected on an endpoint, you create an account policy that applies to new accounts. New account policies run when accounts are detected when the Correlate option is included in the Explore and Correlate definition. If an account was found when running explore only, the policy runs the next time the Correlate option is included when exploring that endpoint.

To create a policy for new accounts

1. In the User Console, click Endpoints, or click Tasks, Endpoints.
2. Reverse New, Create Reverse Sync New Account Policy.
3. Enter a name and description for the policy.
4. Enter the following parameters:
   - Priority—The priority of policy. The highest priority policy is the one with the lowest number. If two policies have the same priority and the same scope, either policy may run. Therefore, be sure to set different priority levels.
   - Endpoint Type—All endpoints or a specific endpoint type.
   - Endpoint—The specific endpoint name. If Endpoint Type is All, the only choice is All endpoints.
   - Container—The container where the account resides. This field applies only to hierarchical endpoints. Enter the container as a list of nodes, ending with the endpoint. For example, for an AD OU with the path "ou=child,ou=parent,ou=root,dc=domain,dc=name" the format "child,parent,root" is correct.
   - Correlated User—Controls when to run the policy based on if a correlated user is found in the Provisioning Directory.

5. Select one of the following Actions:
   - Accept—Takes no action on the account. This choice would be useful if two policies exist, one that rejects all new accounts, and a higher priority policy that accepts accounts created under a certain OU. Therefore, if the account was created at that OU, it is accepted. The reject priority does not run since it has a lower priority.
   - Delete—Removes the account from the endpoint.
   - Suspend—Leaves the account in the endpoint, but suspends it.
   - Send for Approval—Submits the change for workflow approval.
6. Perform the following steps if you set Action to Send for Approval:
   a. Click the icon next to Workflow Process.
   b. Choose a workflow process.
   c. Click OK.
7. Click Submit.

If you assigned a workflow process to the policy, you need to create an approval task (see page 57).

Create a Policy for Modified Accounts

Any account attribute in an endpoint account can be managed by Reverse Synchronization, as long as it is defined in the attribute mapping (see page 51).

To define a process for when a discrepancy is found between existing endpoint accounts and their known values in Identity Management, you can create an account policy that applies to existing accounts. If an attribute is multivalued, more than one value might have been added or removed. In this case, the policy is applied to each value separately or you can create different policies for different values.

To create a policy for modified accounts

1. In the User Console, click Endpoints, pr Tasks, Endpoints.
2. Click Reverse Modify, Create Reverse Sync Modify Account Policy.
3. Enter a name and description for the policy.
4. Enter the following parameters:
   - Priority—The priority of policy. The highest priority policy is the one with the lowest number. If two policies have the same priority and the same scope, either policy may run. Therefore, be sure to set different priority levels.
   - Endpoint Type—All endpoints or a specific endpoint type.
   - Endpoint—The specific endpoint name. If Endpoint Type is All, the only choice is All endpoints.
   - Container—The container where the account resides. This field applies only to hierarchical endpoints. Enter the container as a list of nodes, ending with the endpoint. For example, for an AD OU with the path "ou=child,ou=parent,ou=root,dc=domain,dc=name" the format "child,parent,root" is correct.
   - Attribute—The physical name.
   - Value—A string representation of the value, which may contain ***** (asterisk) as a wildcard. The wildcard refers to any value in the change.

5. Select one of the following Actions:
   - Accept—Updates the account value in the Identity Management user store to match the value in the endpoint account.
   - Reject—Reverts the attribute to reinstate the original value without affecting other changes to attributes for the account.
   - Send for Approval—Submits the change for workflow approval.
6. Perform the following steps if you set Action to Send for Approval:
   a. Click the icon next to Workflow Process.
   b. Choose a workflow process.
   c. Click OK.
7. Click Submit.

If you assigned a workflow process to the policy, you need to create an approval task (see page 57).

Create an Approval Task for Reverse Synchronization

You create reverse approval tasks for policies that have a Send to Workflow action. Consider the following guidelines for creating the tasks:

- For tasks that approve new accounts, you have two choices.
  - You can create a generic approval screen for accounts. The profile screen for the task shows only general information about the account. The Approve Reverse New Account task operates in this manner.
  - If the approver needs to see the details of the new account, that screen must be specific to the endpoint type. So the approval task with the screen should be used only for policies that are specific to that endpoint type. The task must include the Reverse Approval tab.
- For tasks that approve account modifications, the approval screen must be specific to an endpoint type, so that the approver can see the changed values.

Reverse approval tasks are identical to approval tasks used for account changes. If an approval task for a specific endpoint type already exists, that task can be used. For a new account, an additional reverse approval tab is needed. If an existing approval task for the endpoint type does not exist, use the following procedure.

To create an approval task for reverse synchronization

1. In the User Console, click Taks, Roles and Tasks, or click Roles and Tasks.
2. Click Admin Tasks, Create Admin Task.
3. Select the modify task for the endpoint.

   The name would start with modify and state the name of the endpoint type. Modify Active Directory Account is an example.
4. Make the following changes on the Profile tab:
   - Change the name of the new task.
   - Change the task tag.
   - Change the action to Approve Event.
5. Make the following changes on the Tabs tab:
   a. Remove all Relationship tabs.
   b. Add the Reverse Approval tab if the task is to approve new accounts. Move this tab to be the first tab.
   c. Copy and edit the approval screens on the tabs as necessary.

      Note: You may run into problems when using some account screens in an approval task. If so, modify the default account screen for the tab to make it work in the task.
6. Click Submit.
7. If the task is for new account approvals, add the task to a role to which the approver would belong. The role defines the user scope, which is used to search for users to whom the new account can be assigned.

Execute Reverse Synchronization

Reverse synchronization occurs when you use the Execute Explore and Correlate task. Using this task, you update the Identity Management Provisioning store with the new or changed accounts on an endpoint.

To execute reverse synchronization

1. Create an explore and correlate definition that includes a Correlate option. Correlation is needed to detect new accounts.
2. Click Tasks, Endpoints, Execute Explore and Correlate.
3. Choose a definition that applies to the endpoint with the new or changed accounts.

   Note: When correlating to the existing user, the user must exist in the Provisioning Directory, otherwise the user is correlated to the default user in that directory. The Identity Management user store is not in the scope of the Explore and Correlate task.
4. Click Submit.

If a policy has no workflow process, the accounts are already processed as defined in the policy.

Note: If multiple attributes were rejected on an account that was detected by reverse synchronization policy, all actions are put into one event. However, if that event fails due to an issue with one of the attributes, no attributes are updated.

If workflow is part of the policy, any approvals generated by the reverse synchronization appear under Workflow, View My Work List for the approver.

For new accounts, the approver has the following choices:

- The approver may choose to suspend or delete the account in the endpoint, by selecting either Delete or Suspend and then clicking reject.
- Otherwise, the approver may accept the new account by clicking Approve.

  If an approver does not select a user in the Correlated User field, the account is assigned to the default user. If the Correlated User field is populated in the approval task, the account is correlated with this user. The Correlated User field contains the suggested user found by the correlation mechanism if a user can be found.

For modified accounts, the approver has the following choices:

- For each account, the approver sees which values are changed and can approve or reject them just as if the changes were initiated in the account management screens.
- The approver sees changes to capability attributes (such as an Active Directory groups) as separate approval events.

To verify if reverse synchronization succeeded

1. Go to System, View Submitted Tasks.
2. Complete the task name field as follows: Provisioning Activity
3. Click Search.

The results show if the reverse synchronization events completed successfully.

Chapter 2: Deploying a Custom Connector to the Cloud

This section describes how you can deploy a custom connector to the cloud.

If you prepare correctly, you can deploy the following connectors to the cloud connector server:

- Connectors with custom attributes (see page 62): You can add custom attributes to the following connectors that are shipped with CA IAM CS:
  - CA DLP
  - SAP UME
  - ACF2 v2
  - CA Top Secret v2
  - RACF v2
- Custom connectors (see page 63): Any dynamic connector that was created using the following templates in Connector Xpress
  - JDBC
  - JNDI
  - DYN SDK

Note: In CA CloudMinder 1.0, you cannot deploy these connectors to the cloud. If you upgrade from CA CloudMinder 1.0 to a newer version, the connectors in the previous lists are removed during the upgrade process. This allows you to take advantage of the new ability to deploy a custom connector to the cloud.

You **cannot** deploy any custom static connector that was created using the following templates in Connector Xpress:

- SDK (Deprecated)—Use the Role Definition Generator.
- LND—This connector is already deployed.

Deploy a Connector with Custom Attributes

Use this procedure for deploying a connector that was shipped with CA IAM CS and later customized.

Follow these steps:

1. Prepare to deploy connectors with custom attributes:
   a. Enable the relevant admin roles, and ensure that the approving user has at least the following roles:
      - Endpoint Manager
      - Provisioning Synchronization Manager

      If these roles are not enabled, the approval task will not be generated. This would prevent the connector from being deployed.
   b. Enable email notifications.
   c. Enable workflow.
   d. Configure Global policy-based workflow for the following events:
      - CreateEndpointType
      - ModifyEndpointType
      - DeleteEndpointType
2. Add the on-premise connector server to the cloud connector server.
3. Create a route (see page 25) and mark any of the endpoint types as managed by the on-premise connector server.
4. Open Connector Xpress, and follow these steps:
   a. Connect to the Provisioning Server using the Remote Server option.
   b. Access the required endpoint type.
   c. Update something in the metadata. For example, update the version number.
   d. Save the metadata file.
   e. Deploy the connector.
5. The tenant administrator can now log in to the User Console as a user with sufficient roles (defined in Step 1a), then search for the pending approval task and approve it.

The role definition is deployed, and the screens are now available in Identity Management.

Deploy a Custom Connector

You can create a connector with Connector Xpress and then deploy it to a local CA IAM CS. If the deployment is approved, you can then configure it to work in the cloud.

To deploy dynamic connectors in CA CloudMinder, Connector Xpress connects to an on-premise connector server that communicates with a connector server in the cloud. The cloud connector server communicates with a cloud Provisioning Server, which manages endpoint accounts in CA CloudMinder.

Connector Xpress lets you configure metadata settings to a project file and then deploy a connector from that file. For example, you can use a project file when you move connectors from a test environment to a production environment. This project file ensures that you have the same settings in both environments.

Follow these steps:

1. Configure Connector Xpress for CA CloudMinder
2. Create a project.
3. Open the project.
4. Deploy the connector:
   a. In the Provisioning Servers tree, expand the Provisioning Servers node and then choose the server where you want to deploy the connector.
   b. In the Provisioning Server Password Required dialog, complete the fields on the dialog to specify the password for the server, and click then OK.
   c. Expand the server, and then right-click Endpoint Types, then click Create New Endpoint Type.

      The Create New Endpoint Types dialog appears.
   d. To define the name of your new endpoint type, complete the fields on the dialog then click OK.
5. The workflow is triggered. The approver receives a message that you want to deploy a new endpoint type.
   - If the approver rejects the change, nothing further happens. The endpoint type is not deployed.
   - If the approver approves the change, the following steps happen.
6. You receive an email notification that the deployment was approved.
7. You receive another email notification that the deployment was completed. You can now continue setting up the connector.
8. In the User Console, add one or more administrators to an admin role that can manage the endpoint.

   Identity Management creates the role automatically when you deploy the connector. The role name has the following format:

- Provisioning Manager for *your_endpoint_type*

For information on how to assign admin roles, see Assigning Roles.

Remove a Connector

You can use Connector Xpress to undeploy connectors. Undeploying a connector deletes the connector from the Provisioning Server and from CA IAM CS.

When you use Connector Xpress to undeploy a connector, a Delete Endpoint Type task is created.

Important! When an approver rejects a Delete Endpoint Type task, some screens are not removed. We strongly recommend that the approver approves every request to remove an endpoint.

Extend Custom Attributes on Endpoints

The Provisioning Server can manage custom endpoint attributes. To enable Identity Management to read custom endpoint attributes that are associated with provisioning roles, additional steps are required.

To extend custom attributes on endpoints

1. Generate metadata from the parser table if this connector was created before Identity Management r12.5.

   See the *Connector Programming Guide*.

2. Use Connector Xpress as follows:

   a. Install metadata in the namespace node.

   b. Generate a JAR file, property file, and role definition file using the Role Definition Generator.

      For details, see the *Connector Xpress Guide*.

3. Copy the JAR file to this location:
   - (Windows) *app server home*/iam_im.ear/user_console.war/WEB-INF/lib
   - (UNIX) *app server home*\iam_im.ear\user_console.war\WEB-INF\lib

     Note: For WebSphere, copy the JAR file to: WebSphere_home/AppServer/profiles/*Profile_Name*/config/cells/*Cell_name*/applications/iam_im.ear/user_console.war/WEB-INF
4. Copy the property file to this location:
   - (Windows) *app server home*/iam_im.ear/custom/provisioning/resourceBundles
   - (UNIX) *app server home**i*am_im.ear\custom\provisioning\resourceBundles

     Note: For WebSphere, copy the properties file to:

     WebSphere_home/AppServer/profiles/*Profile_Name*/config/cells/*cell_name*/applications/iam_im.ear\custom\provisioning\resourceBundles
5. Repeat the preceding two steps for each node if you have a cluster.
6. Restart the application server.
7. Import the role definition file as follows:
   a. In the Management Console, select the environment.
   b. Select Role and Task Settings.
   c. Click Import.
   d. Select the endpoint type and click Finish.