CA CloudMinder™

Administration Guide

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: Overview

This section contains the following topics:

CA CloudMinder Services

CA CloudMinder ™ is a suite of cloud-based security services that enable organizations to manage user identities and authentication effectively. These services are delivered using the software-as-a-service (SaaS) model, and can be described as follows:

- **Identity Management**

  The *Identity Management* service offers user management and provisioning capabilities. This service enables administrators to control access to system resources such as applications and cloud-based services.

- **Advanced Authentication**

  The *Advanced Authentication* service offers protection against unauthorized access by using a combination of *strong authentication* (also known as *two-factor authentication*) and *risk evaluation*.

  The strong authentication feature verifies an end user's identity using a One-Time Password (OTP) or a Public Key Infrastructure (PKI) credential with a password. Consequently, this type of authentication is harder to compromise.

  The risk evaluation feature provides real-time protection against fraud in online transactions by examining a wide range of data that is collected from the end user and their device. A risk score and advice are generated based on this data and the end user is granted access, denied access, or requested to provide additional authentication.

  You can choose to use two-factor authentication, risk evaluation, or both features.

- **Single Sign-On**

  The *Single Sign-On* service offers secure single sign-on across a network of trusted business partners. This service enables an organization to establish federated partnerships so that an end user who is logged in to one application or portal can access a trusted partner application simultaneously without having to log in again.

CA CloudMinder administrators are responsible for installing, hosting, and managing all the CA products that form the CA CloudMinder solution. An administrator in your organization, who is given the *tenant administrator* role, can perform the configurations and maintenance that your business requires, such as managing end users and their credentials.

Note: For more information, see *CA CloudMinder Overview*.

Basic Capabilities

CA CloudMinder includes the capabilities that are available in all deployments, in addition to service-specific capabilities. You can use these capabilities, regardless of which services your deployment includes.

User Management

- Secure user login and authentication.
- Role-based access control and delegation, which allows administrators to control user access to system resources such as user profiles, applications and cloud-based services.
- User self-registration and forgotten password services.
- Self-management of user profile information.

Entitlement Management

- User self-request, or *access request*, for access to system resources.
- Business policy administration, allowing administrators to write and apply rules that govern user access to system resources, or user *entitlements*, that are based on internal business policies.
- *Workflow control*, allowing administrators to confirm or reject system actions before they take place.

Monitoring & Reporting

- Auditing and reporting, allowing auditors and analysts to confirm that security and business policies are enforced, and to identify potential problems.
- Monitoring, allowing administrators to confirm and manage system uptime.

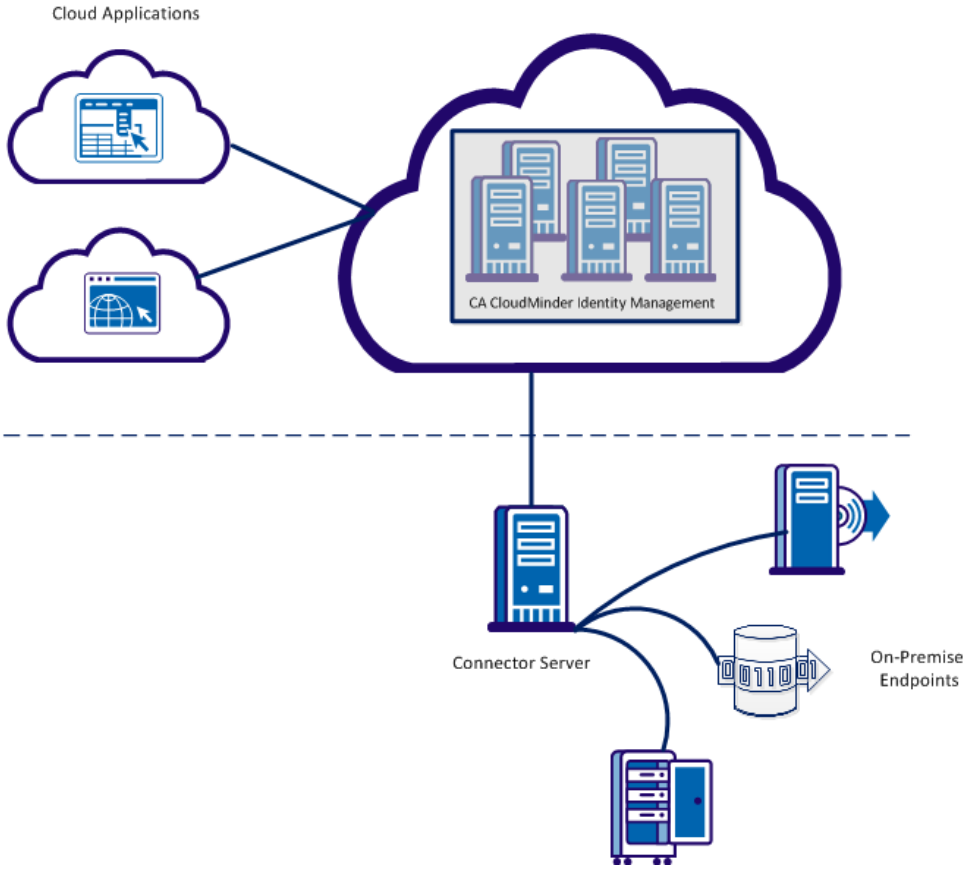
CA CloudMinder Identity Management Service

Identity Management allows you to manage user accounts in on-premise and cloud applications, called *endpoints*, from a single location. Administrators can assign and revoke accounts. Administrators can also specify account settings, such as mailbox size for an email account.

Administrators manage endpoint accounts through *provisioning roles*. Provisioning roles contain account templates, which define account settings. When an administrator assigns a provisioning role to a user, that user receives the accounts defined by the templates in the role.

A provisioning role can manage accounts on multiple endpoints. For example, a Sales provisioning role can include an account for a salesperson in SalesForce.com, a cloud application, and Active Directory, and on-premise application.

Identity Management communicates with endpoints through connectors. To communicate with applications installed in your organization's data centers, you install an on-premise connector server, as shown in the following illustration.



CA CloudMinder Advanced Authentication Service

The CA CloudMinder™ Advanced Authentication service protects your organization's resources against unauthorized access.

Advanced Authentication includes the following features:

- Strong Authentication (see page 13)
- Risk Evaluation (see page 13)

Strong Authentication

Strong authentication addresses the exponential increase in internet-based fraud over the last few years. The basic user name-password model for authentication is no longer sufficient.

Strong authentication uses two-factor authentication, where an end user is required to provide more than one form of identification. For example, in addition to the typical user name-password (something the user knows), the end user also has to provide an additional hardware or software credential (something the user has).

The Advanced Authentication service provides proprietary software credentials, which can be used as the possession factor (something the user has) for authentication. The end user's password or PIN is used as the knowledge factor (something the user knows). As a result, end users retain the familiar user name-password login process. They need to know only their user name and password or PIN, but are protected by a strong authentication solution that works in the background.

The following strong authentication credential types are available to protect resources in your organization:

- ArcotID PKI
- ArcotID OTP

These credential types are discussed in detail in later topics.

Risk Evaluation

When an end user tries to access a protected resource, the Advanced Authentication service first collects a wide range of data, such as details about the following:

- End-user device identification
- Location
- Users and transactions

The service evaluates that data using risk evaluation rules.

A *risk evaluation rule* is a set of conditions against which the end user or device data is validated. The result of each rule is then evaluated in the order of priority that is set by an administrator. A score and advice are generated based on the first rule that matched (the higher the risk score, the greater the probability of a fraud). Based on this advice, the end user is granted access, denied access, or asked for additional authentication.

The risk evaluation rules are listed and explained in a later section.

Single Sign-On Service

CA CloudMinder™ Single Sign-On (SSO) provides a cloud-based federation hub that lets customers connect to cloud-based applications, partner hosted applications or other on-premise applications in an organization.

The SSO service is standards-based. The service uses SAML, WS-Federation, and WS-Trust to securely share user identity information across business partners. Users log in one time and gain secure access to federated partner services and application without the inconvenience of maintaining different access credentials. Federated partnerships are deployed and maintained in the cloud so that your organization does not have to develop the infrastructure internally.

All types of users can single sign-on to a particular site. Users can be enterprise customers, such as employees that work at your company facility or from outside your corporate facility. Enterprise users can also be third-party partners that are not part of your organization. Users can be consumers that enroll in services that a company are offers, such as a rewards program. The SSO service can provide access to applications for these types of customers.

CA CloudMinder Components

CA Directory

CA Directory is an LDAP-based directory server that hosts multiple CA CloudMinder data stores.

CA Directory provides the following functionality in CA CloudMinder:

- User Store

  Contains information about all of the managed users in CA CloudMinder.

  CA Directory can contain millions of users.

- Provisioning Directory

  Contains a representation of users who have accounts on endpoints such as Microsoft Exchange, Active Directory, and SAP. Users in the provisioning directory are called *global users*.

CA Directory securely stores the data of one tenant separately from the data of any other tenant. A tenant can never view or access the data of another tenant. User data and provisioning data is physically segregated into separate server instances, or *DSAs*, for each tenant. Any request that requires user or provisioning data contains information that identifies the request with a specific tenant. A router directs the request to the appropriate DSA.

CA SiteMinder Policy Server

The Policy Server provides the following functionality in CA CloudMinder:

- Authentication—The Policy Server supports a range of authentication methods. It can authenticate users based on user names and passwords, forms based authentication, and through public-key certificates.

  In deployments that include Advanced Authentication, the Policy Server integrates with CA AuthMinder to support strong authentication methods, such as One Time Password (OTP), and Arcot PKI.

- Authorization—The Policy Server is responsible for managing and enforcing access control rules established by the Policy Server administrator. These rules define the operations that are allowed for each protected resource.

- Password policy enforcement—The Policy Server enforces rules and restrictions that govern the following:
  - password expiration
  - composition
  - usage

- Partnership federation—Offers secure single sign-on and single logout across a network of trusted business partners.Partnership federation supports the following profiles:
  - SAML 1.1
  - SAML 2.0
  - WS-Federation Passive Requester

CA SiteMinder Secure Proxy Server

The CA SiteMinder Secure Proxy Server (SPS) is a stand-alone server that provides a proxy-based solution for access control.

The CA SiteMinder Secure Proxy Server uses a proxy engine that provides a network gateway for the enterprise. The SPS provides the following functionality in CA CloudMinder:

- An embedded and fully supported web server, including SSL accelerator card support and a GUI tool for managing keys and certificates
- Support for multiple session schemes (cookie-based, and cookie-less)
- Support for flexible proxy rules, such as the following:
  - Support for rules that are based on HTTP headers and CA SiteMinder responses, in addition to URLs.
  - Ease of use for complex rules.

CA IdentityMinder Server

CA IdentityMinder provides the core functionality of CA CloudMinder, including profile and entitlement management, policies to support business rules, user self-service, and reports. You also perform most provisioning tasks in CA IdentityMinder.

Provisioning Server

The Provisioning Server allows administrators to provision accounts on endpoints such as email servers, databases, and other applications to end users. To communicate with the endpoint systems, you also install connector servers for endpoint-specific connectors, such as an SAP connector.

CA IAM Connector Server

The CA IAM CS manages *connectors*, software that enables communication between CA CloudMinder and an endpoint system. An *endpoint* can be any system that uses identities.

A typical deployment includes the following types of connector servers:

- **Cloud CA IAM CS**

  Directly manages cloud endpoints, such as Google Apps or Salesforce. The cloud CA IAM CS is installed in the host data center.

- **On-premise CA IAM CS**

  Manages local endpoints in an internal network at the tenant site.

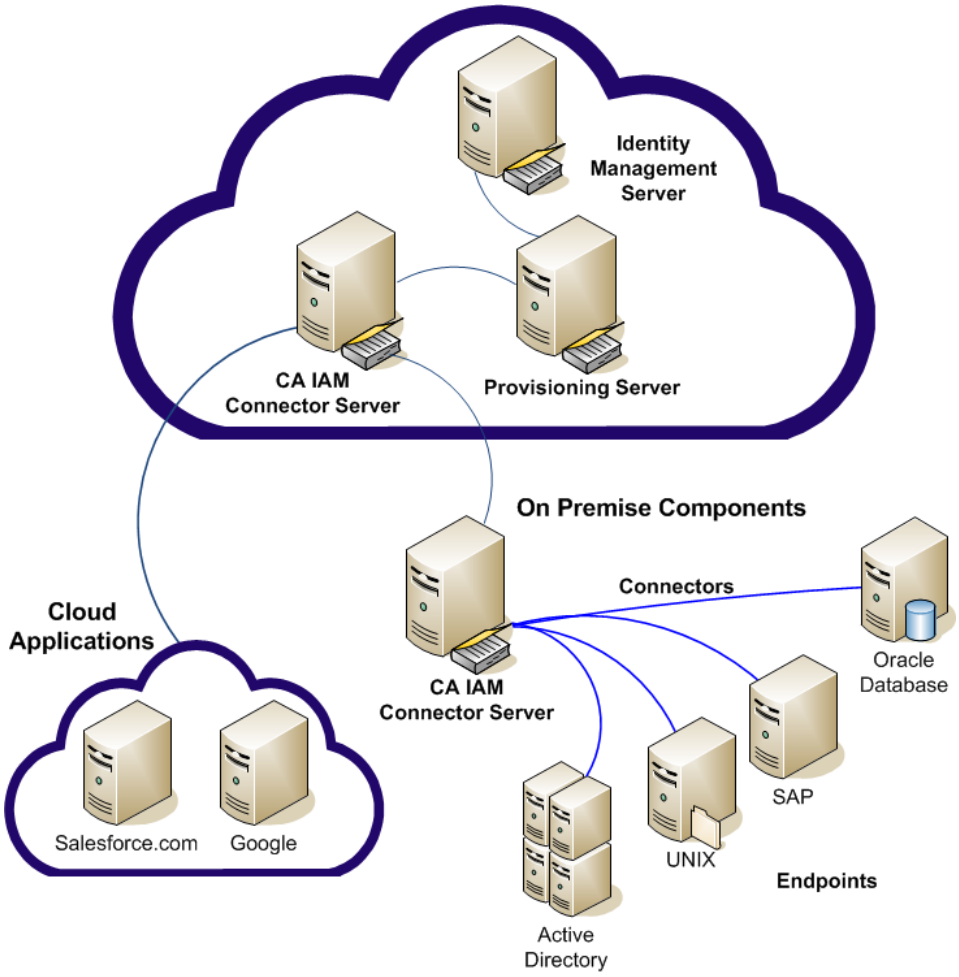
  The tenant administrator can install a local version of the CA IAM CS in their internal network and enable routing from the cloud.

  Note the following requirements for the on-premise CA IAM CS:

  - The on-premise CA IAM CS must access the Cloud CA IAM CS using HTTP/S.
  - The on-premise CA IAM CS must be able to access the on-premise endpoints using traditional communication methods, such as LDAP, CAM/CAFT, and others.

You can add support for new connectors on-premise or in the cloud without restarting any servers.

The following example shows a deployment that includes two cloud endpoints and four on-premise endpoints.


Identity
Management
Server
CA IAM
Connector Server
Provisioning Server
On Premise Components
Connectors
Cloud
Applications
CA IAM
Connector Server
Oracle
Database
SAP
UNIX
Endpoints
Salesforce.com
Google
Active
Directory

CA AuthMinder

In CA CloudMinder, CA AuthMinder provides strong authentication.

Strong authentication uses two-factor authentication, where an end user is required to provide more than one form of identification. For example, in addition to the typical user name-password (something the user knows), the end user also has to provide an additional hardware or software credential (something the user has).

The Advanced Authentication service provides proprietary software credentials, which can be used as the possession factor (something the user has) for authentication. The end user password or PIN is used as the knowledge factor (something the user knows). As a result, end users retain the familiar user name-password login process. They need to know only their user name and password or PIN, but are protected by a strong authentication solution that works in the background.

The available Strong authentication credential types are:

- ArcotID PKI
- ArcotID OTP

CA RiskMinder

CA RiskMinder evaluates end user logins for possible fraud. When an end user tries to access a protected resource, the Advanced Authentication service first collects a wide range of data, such as the following details:

- End-user device identification
- Location
- User and transaction
- The service evaluates that data using risk evaluation rules.

CA RiskMinder evaluates the end user or device data against risk evaluation rules. CA RiskMinder provides a score and advice about the probability of a fraud. Based on this advice, the end user is granted access, denied access, or asked for additional authentication.

Report Server

The Report Server, also known as CA Business Intelligence, generates reports.

The Report Server provides the following functionality:

- Report scheduling
- Default reports, including reports for Advanced Authentication, SSO, and billing
- Support for a report template
- Support for data replication
- Hosting and tenant administrators can request and view reports.

Databases

The components in CA CloudMinder require the following data stores:

- Advanced Authentication application stores
- CA IdentityMinder object store

  Stores information for auditing, task persistence, workflow, and CA IdentityMinder objects.
- Reporting store

  Uses CA Business Intelligence 3.2. You use this server to include data from the Snapshot Database, which contains information from the CA IdentityMinder Object Store and the CA IdentityMinder user store. An example of a Snapshot Report is the User Profile report. You can also create reports with a disabled snapshot applied, which include data from other data sources, such as the Audit Database.
- SiteMinder policy store, session store and key store

Consoles

Administrators use the following UIs to configure and manage CA CloudMinder:

- User Console
- CSP Console
- Management Console
- Advanced Authentication Administration Consoles

Administrative UI

The Administrative UI is a version of the SiteMinder Administrative UI that includes tenant management tasks. Hosting administrators use the Administrative UI to complete the following tasks:

- Create and manage a tenant deployment
- Configure federation partnerships

Tenant administrators do not have access to this console.

The Administrative UI is web-based. The URL for accessing the Administrative UI resembles the following:

http://*hostname:port*/iam/siteminder/console

hostname

Defines the fully qualified domain name or IP address for the server where CA SiteMinder is installed.

port

Defines the application server port.

Note: Administrators must provide valid credentials to access the Administrative UI. The Administrative UI validates the credentials against the CA Directory user store.

Management Console

The Management Console allows hosting administrators to manage CA IdentityMinder directories and tenant environments. Use the Management Console to configure the initial roles in the system, and to enable certain advanced features.

The Management Console is installed with the Identity Management server (CA IdentityMinder).

To access the Management Console, enter the following URL in a browser:

http://*hostname:port*/iam/immanage

hostname

Defines the fully qualified domain name or IP address for the server where CA IdentityMinder is installed.

port

Defines the application server port.

Tenant administrators do not have access to the Management Console.

User Console

Tenant and hosting administrators use the User Console to manage a tenant environment.

The User Console includes a set of default tasks and admin roles.

- Tasks are actions that administrators or end users perform in CA CloudMinder.
- Admin roles associate users and privileges. A user who has a role can perform its tasks. Users may have multiple roles. For example, a user may have the roles accountant and employee.

  Tenant and hosting administrators have different roles. They can perform different tasks for an environment.

After you create an environment, you can access it by typing a URL in a browser.

The format of the URL depends on how you configured the environment and the type of task that you want to access.

- To access protected tasks from the User Console, use the following URL:

  https://*hostname*/*iam*/im/*alias*

  hostname

  Defines the fully qualified domain name of the SPS system or the IP address of the SPS loadbalancer.

  alias

  Defines the alias of the tenant.

Note: All CA IdentityMinder tasks are protected unless you configure public tasks.

- To access public tasks, which do not require users to provide credentials, use a URL with the following format:

  https://*hostname*/iam/im/*alias_pub*/index.jsp?task.tag=*tasktag*

  hostname

  Defines the fully qualified domain name of the SPS system or the IP address of the SPS loadbalancer.

  alias

  Defines the alias for public tasks.

  task_tag

  Defines the tag for the task to invoke.

  You specify the task tag when you configure a task in the User Console.

  The task tags for the default self-registration and forgotten password reset tasks are SelfRegistration and ForgottenPasswordReset.

Advanced Authentication Administration Consoles

CA CloudMinder includes two consoles for advanced authentication. Hosting administrators use the master admin console to create a global admin, and to refresh cache. Global admins use a separate console to configure CA AuthMinder and to refresh certain caches.

Tenant administrators do not access this console.

The URL for the Advanced Authentication Administration consoles resembles the following:

- Master console:

  http://*hostname:port*/arcotadmin/mabamlogin.htm

- Global admin console:

  http://*hostname:port*/arcotadmin/adminlogin.htm

What Can I Do with CA CloudMinder?

The following sections describe the features and functionality in CA CloudMinder.

Users and Services They Need

The typical Information Technology (IT) department faces a constant demand to maintain user accounts. IT administrators must address urgent needs of users, such as resetting forgotten passwords, creating new accounts, and providing supplies and office equipment.

Simultaneously, IT administrators must provide users with access to services. For example, a department manager generates purchase orders and needs an account in a financial application. Other users may need access to salesforce.com and Microsoft Exchange.

To address the escalating demands on IT, Identity Management provides an integrated method of managing users and their access to services, including:

- Assignment of privileges through roles. Specifically:
  - Roles that enable administrators to create and maintain user accounts
  - Roles that provision additional accounts to existing users

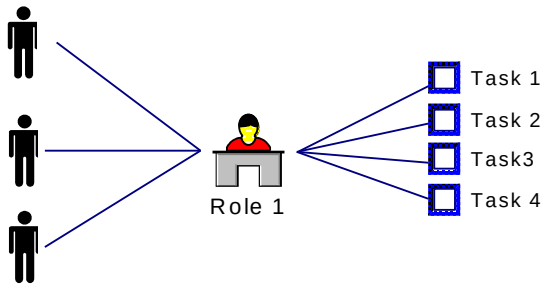
- Assignment of services that contain roles, groups, and tasks that meet a typical business role
- Management of rules for creating and update passwords
- Self-service options so users can manage their own accounts

Manage Users with Admin Roles

In Identity Management, you manage users through admin roles. For example, you use admin roles to modify profile attributes of users, give users options for managing their own accounts, and to approve tasks that use workflow.

Roles simplify privilege management. Instead of associating a user with each task that he performs or each account that he needs, you can assign a role to the user. The user can perform the tasks in the role or can use the accounts that are associated with the role. Tasks enable users to perform Identity Management functions, such as modifying a profile.

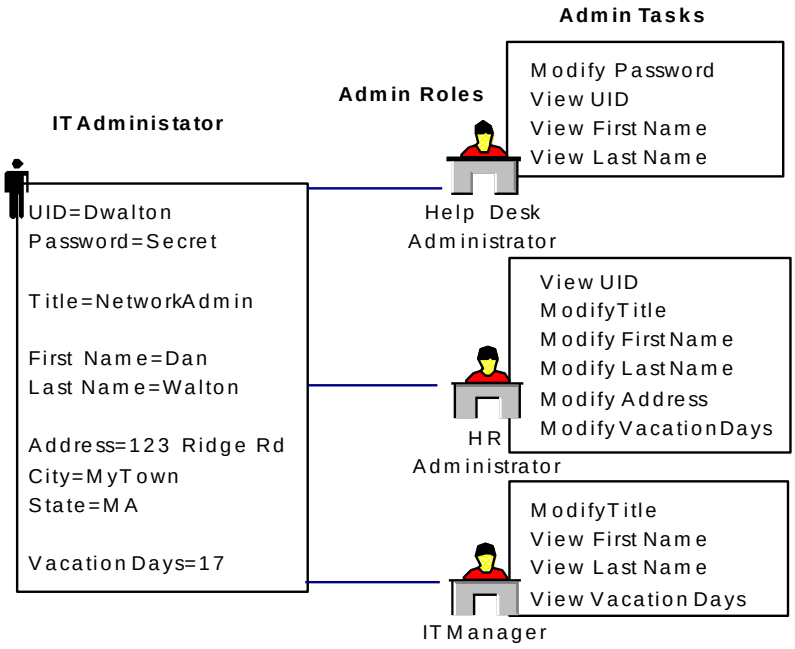
The following illustration shows several tasks which are combined into a single admin role and assigned to multiple users:



You also use admin roles to manage other user store objects (groups and organizations) and to manage the roles and tasks through which you manage user store objects.

Profile Management at the Attribute Level

You can create admin roles for different administrators who need to read or write different profile attributes. For example, a company may have several employees who perform operations on user profiles, each accessing different attributes. The following figure shows three roles and their associated tasks. Each role has different access to profile attributes.



In this example:

- A Help Desk administrator views user names and addresses and resets user passwords.
- A Human Resources administrator modifies user IDs, user names, addresses, titles, and number of vacation days.
- An IT manager modifies the title of users and views their name and number of vacation days.

Another administrator could handle the creation and maintenance of groups. So that administrator needs a role with group tasks. Whatever roles you have when you log in to Identity Management, a series of tasks appear based on the admin role assigned to your Identity Management account.

Workflow Approval of Admin Tasks

To help automate business processes, you can design an admin task to generate a workflow process. A *workflow process* automates a well-defined procedure that a company repeats frequently.

Workflow processes are triggered by Identity Management events which are part of an admin task. For example, the Create User task includes events called CreateUserEvent and AddToGroupEvent. When an event occurs, the workflow engine can:

- Require approvals--An approver must approve an event, such as modifying a user profile, before Identity Management updates a user store. Approvers are administrators who have the Approver role for a particular task.
- Send notifications--The workflow engine can notify users of an event's status at different stages of a process, such as when a user initiates an event or when an event is approved.
- Generate work lists--Work lists specify the tasks that a particular user must perform. The workflow engine updates administrators' work lists automatically.

More Access with Services

Services simplify entitlement management. Services allow an administrator to combine user entitlements into a single package, which are managed as a set. The bundle include all the tasks, roles, groups, and attributes that are required by a user for a given business role.

For example, all new Sales employees need access to a defined set of tasks and accounts on specific endpoint systems. They also need specific information added to their user account profiles. An administrator creates a service named Sales Administration, containing all the required tasks, roles, groups, and profile attribute information for a new Sales employee. When an administrator assigns the Sales Administration service to a user, that user receives the entire set of roles, tasks, groups and account attributes defined by the service.

Self Service Options for Users

To further reduce the IT workload, Identity Management includes features for registering new users and supplying a forgotten password. These features require no administrator involvement. The user gains access to Identity Management through a *public console*, which requires no login account. Through this console, a user can self-register at a site or request a reminder about a forgotten password.

To save the time of IT administrators, Identity Management users can manage their own accounts. Because users have a self-management role, they can:

- Maintain personal information
- Change their own password
- Join self-subscribing groups

Password Management

Identity Management includes the following features for managing user passwords:

- Password Policies—These policies manage user passwords by enforcing rules and restrictions governing password expiration, composition, and usage.
- Password Managers—Administrators who have the Password Manager role can reset a password when a user calls the Help desk.
- Self-Service Password Management—Identity Management includes several self-service tasks that allow users to manage their own passwords. These tasks include:
  - Self Registration—Users specify a password when they register at a corporate web site.
  - Change My Password—Users can modify their passwords without help from IT or Help Desk personnel
  - Forgotten Password—Users can reset or retrieve a forgotten password after Identity Management verifies their identity.
  - Forgotten User ID—Users can retrieve a forgotten user ID after Identity Management verifies their identity.

User Types in CA CloudMinder

In a CA CloudMinder environment, the following types of users are common:

- **System administrator** — Manages the CA CloudMinder service for multiple customers. In a typical environment, there are two types of system administrators:
  - **Hosting administrator** — Responsible for installing CA CloudMinder, updating the system, and monitoring performance. Hosting administrators also schedule and execute tasks, such as importing large user populations, that can affect system performance.

    A hosting administrator typically has the Cloud Service Provider (CSP) administrator role, which includes most of the default tasks in the system.
  - **Service administrator** — Responsible for creating and managing tenant environments for a hosted service. System administrators work with tenants to set up an environment initially, including customizing the environment to address business needs, and to implement environment changes over time.

    System administrators typically have the Managed Service Provider (MSP) administrator role.
- **Tenant Administrator** — Manages a tenant environment. The Tenant Administrator manages users, groups, and organizations. Additionally, this user can provision accounts and assign services to end users.

  The Tenant Administrator typically has the tenant administrator role.
- **End user** — Uses CA CloudMinder to manage profile information, including passwords. End users can also request access to a *service*, a collection of entitlements, including tasks, roles, groups, and attributes, needed for a given business role.

  End users typically have the self manager and self password manager roles. Two types of end users exist:
  - Employee — The user registers to gain access to the tenant console or the user is assigned access by a human resources application.
  - Consumer — The user registers using a social network, such as Facebook or Google.

Chapter 2: Tenant Management

This section contains the following topics:

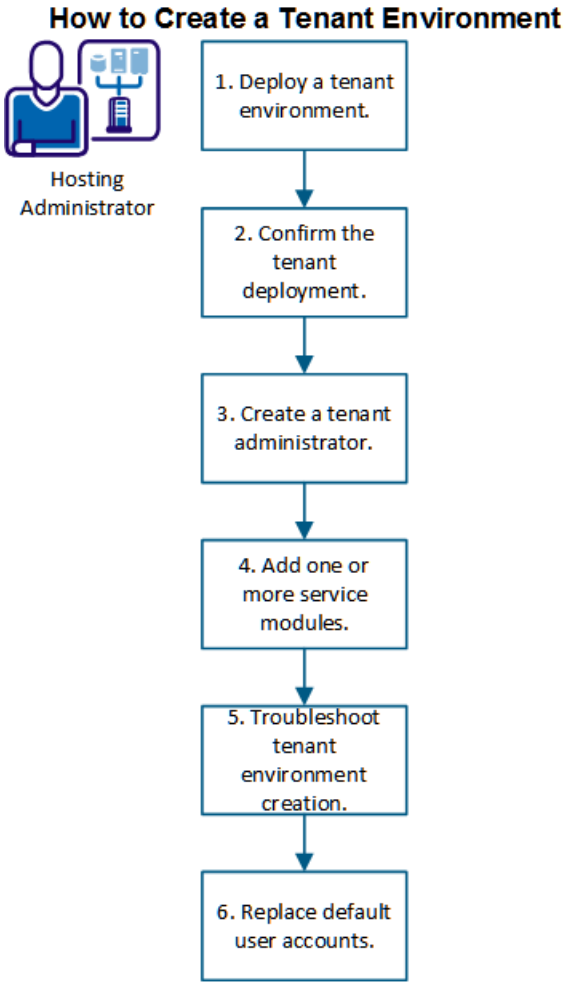
How to Create a Tenant Environment

As a Hosting administrator, you can create an environment for each of your customers named *tenants*. Each tenant environment contains a complete instance of CA CloudMinder. An instance includes the entire suite of system components, servers, user stores, and databases, all specific to that tenant. After you deploy a tenant environment, you or a tenant administrator can alter the environment to meet custom specifications.

Conceptually, tenant environments are part of a three-tier architecture. The first tier is the *hosting environment.* A hosting environment is the virtual environment in which you are running CA CloudMinder. The second tier is the *hosting container.* A hosting container is an object in the hosting environment defined to include everything necessary to run a specific application. The third tier is the tenant environment.

The following diagram shows the steps that you perform to create a tenant environment:

Figure 1: How to create a tenant environment



1. Deploy a tenant environment (see page 33).
2. Confirm the tenant deployment (see page 36).
3. Create a tenant administrator (see page 37).
4. Add one or more service modules (see page 38).
5. Troubleshoot tenant environment creation (see page 40)
6. Replace default user accounts (see page 42).

Deploy a Tenant Environment

When you deploy a tenant environment, the hosting environment creates all the components that are required for the tenant. This process presupposes a defined hosting environment and hosting container, which are established during the CA CloudMinder installation.

Note: Creating or deploying a new tenant restarts the following router DSAs:

- The <HOST-Name>-cam-tenant-router DSA on the Identity Manger server
- The <HOST-NAME>-cam-tenant-router DSA on the SiteMinder Policy server
- The <HOST-NAME>--cam-tenant-router DSA on the Connector server
- The <HOST-NAME>-cam-tenant-router DSA on the Identity Manger Provisioning server
- The <HOST-NAME>-imps-router DSA on the Identity Manger Provisioning server

Follow these steps:

1. Log in to the Administrative UI.
2. Verify that the Environment Base URL uses HTTPS by completing the following steps:
   a. Select Tenants, Manage Hosting Containers.
   b. Select Actions, Modify Hosting Container.
   c. On the Container Profile tab, verify that the Environment Base URL starts with https.

      If the URL begins with http, change the protocol to https, then click Submit.
3. Select Tenants, Manage Tenants.

   A list of tenant that you can administer appears.
4. Click the Create Tenant button.

   The Create Tenant screen appears.
5. Specify the following information for the tenant:

   Hosting Container

   The name of the hosting container created at installation.

   Name

   A friendly name for the tenant.

Tag

A unique identifier for a tenant. The tag is never changed, even if the tenant name changes. Tags can only contain lowercase, alphanumeric, and underscore characters; it cannot start with a number. For example, enter bestcola.

State

A flag that specifies whether the tenant is available for use. When you select Deploy, the system begins the process of deployment as soon as you save the tenant specification. The state displays as Deploying until the process of deployment completes, and then the state changes to Active.

When the state is Inactive, nothing is deployed. In this state, you are editing the tenant data record. You can deploy a saved tenant environment at any time.

Description

A description for the tenant.

Logo

The file location for the tenant logo graphic. The tenant logo graphic appears in the upper-left corner of the Tenant Console. You select a file that is accessible from the local host. The file is uploaded to a system server database.

Protected URL path

A unique name that appears in the URL for accessing protected tasks in the tenant environment.

The private alias name that you enter is appended to the base URL defined during container creation. The combination of the base URL and the private alias forms the URL address where the private environment for this tenant is located. We recommend that you enter the exact value of the tenant tag.

For example, if you enter bestcola as the environment private alias, the tenant private URL becomes:

https://<hostname>/iam/im/bestcola

Users who use this URL to access the tenant environment are required to provide valid login credentials.

Public URL path

A unique name that appears in the URL for accessing public tasks in the environment. Public tasks do not require credentials. For example, a user who does not yet have an account can request one by using a public task.

The public alias name that you enter is appended to the base URL defined during container creation. The combination of the base URL and the public alias forms the URL address where the public environment for this tenant is located. We recommend that you use the following format:

public/<tag>

Tag is the exact value of the tenant tag.

For example, if you enter public/bestcola as the environment public alias, the tenant public URL becomes:

https://<hostname>/iam/im/public/bestcola

DSA Management Username

The DSA management web services user name that is specified during installation of the directory servers.

DSA Management Password

The DSA management web services password that is specified during installation of the directory servers.

Tenant DSA Router Management Username

The DSA management web services user name that is specified during the installation of the directory router servers. Specify this value only when it is different from the directory servers.

Tenant DSA Router Management Password

The DSA management web services password that is specified during the installation of the directory router servers. Specify this value only when it is different from the directory servers.

IMPS DSA Management Username

The DSA management web services user name during the installation of the policy servers. Specify this value only when it is different from the directory servers.

IMPS DSA Management Password

The DSA management web services password that is specified during the installation of the policy servers. Specify this value only when it is different from the directory servers.

IMPS Tenant Service Username

The user name for the web service that is used to deploy tenant provisioning directories. The default is admin, unless this value changes after the installation of the policy servers.

IMPS Tenant Service Password

The password for the web service that is used to deploy tenant provisioning directories. This password is the same as the connector server password specified during the installation of policy servers.

Admin Password

The password for a system administrator account through which you can administer the tenant environment. The user name for this administrator account is automatically set to cspadmin.

6. Click Submit.

   When active, a tenant environment, deployed with a single user, is available for you to log in. The URL has the following format:

   ```
   <hosting container env base url>/<tenant env alias>
   ```

   The user name is cspadmin; the password is the administrator password that was specified when the tenant was deployed. You can log in to the environment and can create a named user account for a Tenant administrator.

Confirm the Tenant Deployment

After you create a tenant, you can confirm that the tenant deployed successfully in the specified container.

Follow these steps:

1. Select Tenants, Manage Tenants in the Administrative UI.

   A list of tenants you can administer appears.

2. Select the View Tenant action for the new tenant.

   The View Tenant screen appears.

3. Examine the State field.

   - If the tenant creation and deployment are currently in process, the state is Deploying. This process can take as long as 10 minutes. To view the updated state, refresh this screen every few minutes
   - If the tenant is successfully deployed, the state is Active.
   - If the tenant is not successfully deployed, the state is Failed Deployment.

4. If the state is Failed Deployment, examine the Deployment Status field.

   An error message identifies the step in the process that failed, and the specific problem that occurred. For example, the process can fail during the creation of the user directory, because the user directory host name in invalid.

   Correct the identified problem, then deploy the tenant again by selecting the Modify Tenant action and updating the State field.

Create a Tenant Administrator

This procedure presupposes that a tenant environment has been deployed from the Administrative UI.

Follow these steps:

1. Access the User Console for the tenant environment. The URL for the environment has the following format:

   http://hostingcontainer/iam/im/<tenant env alias>

2. Log in to the tenant User Console under the name cspadmin, using the administrative password for the tenant environment.
3. Create a user.
4. Assign the Tenant Administrator role to the user.

   The designated tenant administrator receives an email with the URL of the tenant console, a user id, and a temporary password.

The Tenant administrator is fully deployed in the tenant environment.

Add One or More Service Modules

To provide users with access to one or more of the CA CloudMinder services, you add one or more admin roles using the Enable/Disable Admin Role task in the User Console as described in the topics that follow. Removing a service is essentially the reverse process, that is, clear the specified admin roles.

The tenant administrators for this environment receive email notification any changes in the status of a service.

Enable Identity Management

Enable the Identity Management service for the tenant environment as the CSP administrator.

Follow these steps:

1. Log in to the User Console under the name cspadmin, using the administrative password for the tenant environment.
2. Select Policy Xpress, Enable/Disable Policy Xpress Policy.
3. Select Create provisioning User.
4. Click Submit.
5. Select Roles and Tasks, Admin Roles, Enable/Disable Admin Role.
6. Select the following Admin roles for the Identity Management service:
   - Endpoint Manager
   - Tenant Provisioning Manager
   - Provisioning Role Manager
   - Provisioning Role Membership Approver
   - CSP Provisioning Manager
   - MSP Provisioning Manager
7. Click Submit to save your selections.

The Identity Management service is enabled.

Enable the Single Sign-On Service

To enable the Single Sign-On service, you select the Single Sign On Manager admin role.

Follow these steps:

1. Log in to the User Console.
2. Select Roles and Tasks, Admin Roles, Enable/Disable Admin Role.
3. Select the Single Sign On Manager admin role.
4. Click Select to save your selection.

The Single Sign-On service is enabled.

Enable Advanced Authentication

After tenant deployment, CA AuthMinder automatically generates an organization corresponding to the tenant. If you intend to enable Advanced Authentication, immediately after you deploy the tenant and again after the credential profiles are configured, refresh the AuthMinder cache. See Refresh the AuthMinder Cache for instructions.

To enable the Advanced Authentication service, you first select the Advanced Authentication Manager admin role, and then add the Credential Enrollment task to the Self Manager role.

Follow these steps:

1. Log in to the User Console.
2. Select Roles and Tasks, Admin Roles, Enable/Disable Admin Role.
3. Select the Advanced Authentication Manager role.
4. Click Select to save.
5. Select Roles and Tasks, Admin Roles, Modify Admin Role.
6. Search for the Self Manager admin role.
7. Select Self Manager.

   The Modify Admin Role: Self Manager screen opens.
8. Click the Tasks tab.
9. Select Home from the Filter by category list.
10. Select Credential Enrollment from the Add Task list.
11. Click Submit.

    The Credential Enrollment task is added to the Self Manager admin role.

Advanced Authentication is enabled.

Troubleshoot Tenant Environment Creation

The following sections describe issues that can occur in tenant deployment.

Message: 31003::UDS Restart needed

Symptom:

The following message appears when you deploy a tenant environment:

Message: 31003::UDS Restart needed

Solution:

Restart Tomcat, RiskFort and WebFort on all of the SMPS servers in the installation.

ArcotID PKI Authentication Fails

Symptom:

ArcotID PKI Authentication fails and an error that states a user or org is not found appears in the log.

Solution:

Restart Tomcat, RiskFort and WebFort on all of the SMPS servers in the installation.

Error Configuring Credential Types

Symptom:

After creating a tenant organization, the organization may not be available when configuring authentication credentials.

Solution:

Restart the RiskFort and WebFort servers and continue your authentication configuration task.

Replacing Default User Accounts

A system administrator initially creates a CA CloudMinder tenant environment. At that time, various default administrator accounts are created in the environment, including the following accounts:

User ID	Administrator Type
cspadmin	System or Hosting administrator
mspadmin	System or Service administrator
admin	Tenant administrator

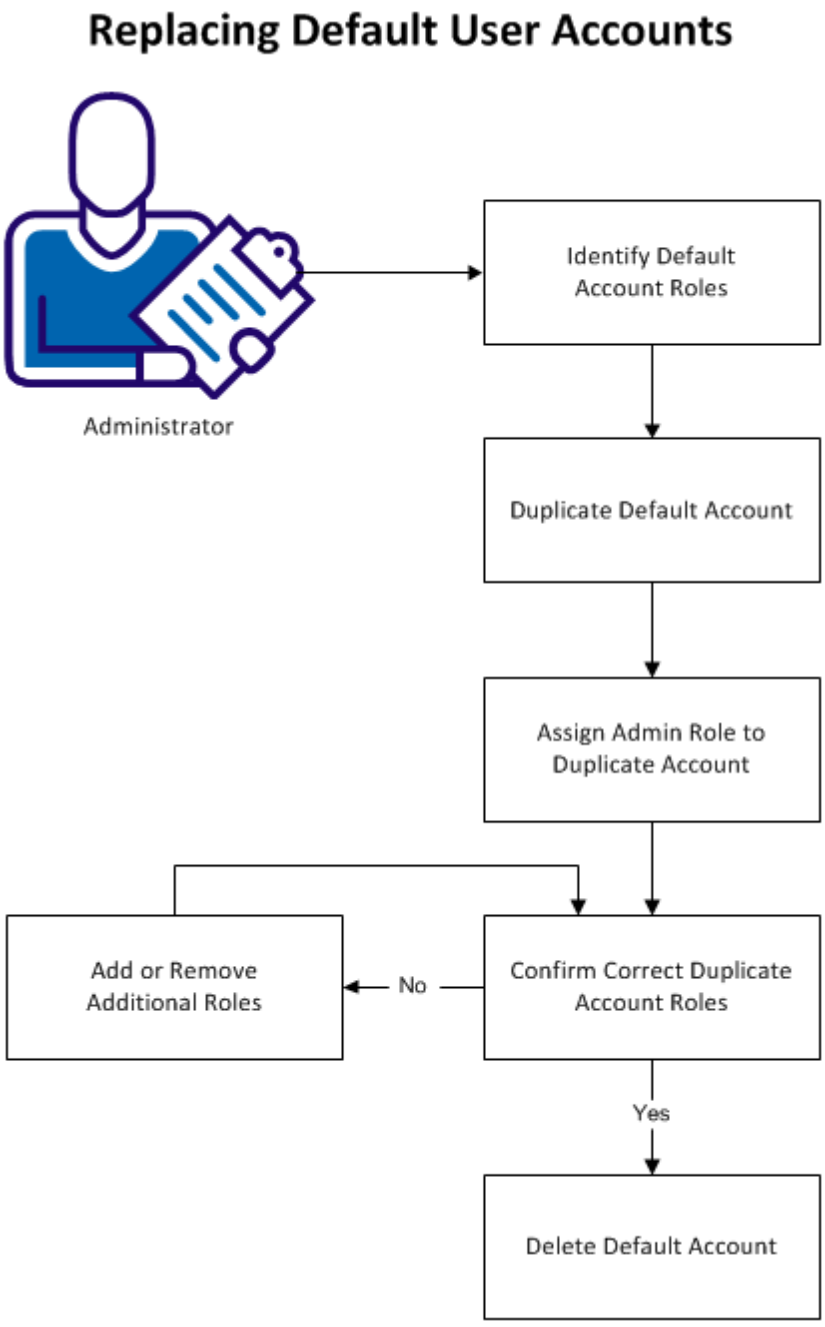
The system creates these accounts with identical passwords. A system administrator typically uses these accounts during the initial configuration of a new tenant environment. Various types of administrators also use these accounts over time to perform configuration and maintenance for the CA CloudMinder environment.

For security reasons, we recommend that upon initially logging in to a default administrator account, you create a duplicate of that account with a unique User ID and password. After you have created the duplicate account, delete the default account.

Replace the default account that corresponds to the type of administrator role that you fulfill. For example, if you are a hosting administrator, replace the cspadmin default account.

Note: Do not replace or delete default accounts that do not correspond to an administrator role that you fulfill. For example, if you are a tenant administrator, do not replace or delete the cspadmin account. If you do so, other types of administrators are unable to log in with those accounts to perform configuration and maintenance for your environment.

The following diagram shows the information to understand, and the steps to perform, in replacing default user accounts.



The following topics explain how to replace default user accounts:

1. Identify the roles that are associated with your default account (see page 44).
2. Duplicate your default account (see page 45).
3. Assign the appropriate admin role to the duplicate account (see page 46).
4. Confirm that the duplicate account contains the correct roles (see page 47).
5. (Optional) Add or remove additional roles, if necessary. (see page 47)
6. Delete the default account (see page 48).

Identifying User Account Roles

Identify the roles that are associated with your default account, so you can accurately duplicate them in your replacement account.

Follow these steps:

1. Log in to your default account, as follows:
   - If you are a hosting or system administrator responsible for tasks in the cspadmin role, log in to cspadmin.
   - If you are a service or system administrator responsible for tasks in the mspadmin role, log in to mspadmin.
   - If you are a tenant administrator, log in to admin.

   Use the password that your system administrator designated to your default account during environment creation.
2. From the navigation menu select Users, Manage Users, View User.

   A search screen appears.
3. Search for the default user account that corresponds to the type of administrator role you fulfill, as follows:

User Account	Administrator Type
cspadmin	System or hosting administrator
mspadmin	System or service administrator
admin	Tenant administrator

4. Select your default user account, and click Select.
5. Click the Admin Roles tab.

   A list of admin roles that are assigned to the user account appears.

6. Note each admin role, and whether you are a Member, Administrator, or both.

   Note: In the cspadmin account, ignore the System Manager role. It is not necessary to duplicate this role when you create the replacement account.

7. Duplicate your default account (see page 45).

Duplicating your Default Account

Create a duplicate account that is based on your default administrator account.

Follow these steps:

1. From the navigation menu, select Users, Manage Users, Create User.
2. Select Create a copy of a user, and search for your default user account, as follows:

User ID	Administrator Type
cspadmin	System or Hosting administrator
mspadmin	System or Service administrator
admin	Tenant administrator

3. Select your default user account, then click Ok.

   The user account profile appears.

4. Enter a new User ID, update any other user profile information, and click Next.

   Note: Do not alter the Organization.

   The groups screen appears. The system automatically duplicates the groups contained in the default account.

5. Click Finish.

   The system creates the user account. The account contains the correct groups, but does not yet contain the correct roles.

6. Assign the appropriate admin role to the account. (see page 46)

Assigning Admin Roles

Assign the appropriate admin roles to the duplicate account.

Follow these steps:

1. From the navigation menu, select Users, Manage Users, Modify User.

   A search screen appears.

2. Search for the User ID of the duplicate account you created.

3. Select the account, and click Select.

   The user profile screen appears.

4. Click Next, then Next again to display the Admin Roles screen.

5. Click Add an Admin Role.

   A search screen appears.

6. Search for the admin role that corresponds with your default user account, as follows:

User ID	Admin Role
cspadmin	CSP Administrator
mspadmin	MSP Administrator
admin	Tenant Administrator

7. Select the role, and click Select.

   An updated list of the roles that are assigned to the account appears.

8. Click Finish.

   The system assigns the role to the account.

   Note: When you assign one of the Administrator roles to an account, the system automatically assigns several related roles at the same time. This configuration ensures that all required privileges are assigned to the account simultaneously.

9. Confirm that the new account contains the correct roles (see page 47).

Confirming User Account Roles

Before you delete your default user account, confirm that the roles assigned to your duplicate account match the roles in the default account.

Follow these steps:

1. From the navigation menu, select Users, Manage Users, View User.

   A search screen appears.

2. Search for the User ID of the duplicate account you created.

3. Select the account, and click Select.

   The user profile screen appears.

4. Click the Admin Roles tab.

   A list of admin roles that are assigned to the user account appears.

5. Confirm that the roles and associated privileges (Member, Administrator, or both) match those you noted when you identified the roles that are associated with your default account (see page 44).

   Note: For the duplicate cspadmin account, ignore the System Manager role. It is not necessary to duplicate this role in the replacement account.

6. If the roles do not match, add or remove roles to match the default account. (see page 47)

7. If the roles match, delete the default account (see page 48).

Adding or Removing Additional Roles

If the roles assigned to your duplicate account do not match the default account, add or remove additional admin roles.

Follow these steps:

1. From the navigation menu, select Users, Manage Users, Modify User.

   A search screen appears.

2. Search for the User ID of the duplicate account you created.

3. Select the account, and click Select.

   The user profile screen appears.

4. Click Next, then Next again to display the Admin Roles screen.

5. To add a role, click Add an Admin Role, search for and select the role, and click Select.

   An updated list of the roles that are assigned to the account appears.

6. To remove a role, uncheck the Member and Administrator checkboxes next to the role.

7. Click Finish.

   The system assigns or removes the role.

8. Confirm that the new account contains the correct roles (see page 47).

Delete the Default Account

You have confirmed that the duplicate account you created matches your default account. You can now delete the default account.

Important! The mspadmin account is the default Inbound Administrator. The system uses the Inbound Administrator to create users during the Explore and Correlate process. Before deleting the mspadmin account, update the Inbound Administrator from mspadmin to a different user account. You must have access to the Management Console to do this. In the Management Console, select Environment, then your environment, and navigate to Advanced Settings, Provisioning.

Follow these steps:

1. Log out of CA CloudMinder.
2. Log in to the duplicate account you created.
3. From the navigation menu, select Users, Manage Users, Delete User.

   A search screen appears.

4. Search for your default account, which is one of the following accounts:
   - cspadmin
   - mspadmin
   - admin
5. Select your default account, and click Select.
6. Confirm that you want to delete the account by clicking Yes.

   The system deletes the default account.

   The process of replacing your default user account is now complete. This process helps prevent improper login attempts on your system.

   You can now use the duplicate account that you created to perform all administrative functions that were associated with the default role.

Delete a Tenant Environment

When you delete a tenant, all components of the tenant are permanently removed, including all provisioning stores, user stores, directories, and databases. The tenant is unregistered from the provisioning server, and deleted from the environment. Any ports that were assigned for use by the tenant are available again. Tenant data is backed up, so that you can recreate a tenant if required.

During deletion, the tenant tag is removed from the system. You can later create another tenant environment with the same name and tag.

Any partnerships created through the Single Sign-on service are not removed when you delete the tenant environment.

Important: When you delete a tenant environment after the Identity Management service has already been removed, be sure to enable Provisioning for the tenant from the Management Console before removing the tenant.

Follow these steps:

1. Delete the environment (only from one Identity Management server)
   a. Access the Management Console

      <Host>:8080/iam/immanage/
   b. Click Home, Environments.
   c. Select the environment for the tenant to be deleted.
   d. Select delete.
2. Delete Directory from the Management Console (only from one Identity Management server)
   a. Access the Management Console
   b. <Host>:8080/iam/immanage/
   c. Click Home, Directories.
   d. Select the checkbox before the directory for the tenant to be deleted.
   e. Click Delete.

      You will not observe any change on the screen.
3. In the Policy Server, navigate to /opt/CA/siteminder/log.
   a. Edit the smps.log file and locate an entry similar to the following:

```
"[Delete.cpp:338][Reduce][ERROR][sm-xpsxps-03340] Cannot
delete a related record.
(CA.SM::UserDirectory@0e-000621de-79d1-1485-8f37-38450a82d0
cb(cm3Tenant
Directory):CA.SM::IMSDirectory@32-00074f6b-79d1-1485-8f37-3
8450a82d0cb(cm3 Tenant
Directory).CA.SM::IMSDirectory.UserDirectoryLink)"
```

b. In this example, the tenant user directory could not be deleted because it had a related entry :
`CA.SM::IMSDirectory@32-00074f6b-79d1-1485-8f37-38450a82d0cb`
.

4. Delete the related entry from Policy Server by following these steps:
   a. Run XPSExplorer.
   b. Type F to find by XID.
   c. Paste the XID obtained from log (CA.SM::IMSDirectory@32-00074f6b-79d1-1485-8f37-38450a82d0cb)
   d. Press enter. The related object is displayed.
   e. Press D to delete the object.
5. Now that the related entry is deleted, delete the user directory from the Management Console by following step 2.
6. If the domain and directory still exist in SiteMinder, restart or reboot SiteMinder services.
   a. On Policy Server

      service S98sm stop

      Service S98sm start
   b. On the Administrative UI:

      service S98smAdminUI stop

      Service S98smAdminUI start
7. Update the tenant DSA router on each Identity Management server, CA IAM CS, Provisioning Server, Policy Server to remove the tenant. Perform the following steps:

   su – dsa

   cd /opt/CA/Directory/dxserver/config/knowledge
   a. Edit the <hostname>-cam-tenant-router file.
   b. For example if cm3 is the tenant, delete the lines with cm3:

```
# CA DXserver/config/knowledge/
#
# Knowledge configuration file written by dxagent
#
```

```
# Refer to the Admin Guide for the format of the set dsa command.

set dsa "s010130009046-cam-tenant-cm3" =
{
prefix =   <o ca><ou cam><ou cm3>
dsa-name =   <o ca><ou cam><ou cm3><cn
s010130009046-cam-tenant-cm3>
dsa-password            = "secret"
address         = ipv4 "s010130009046" port 50006
disp-psap               = DISP
snmp-port               = 50006
console-port            = 50007
auth-levels             = clear-password
dsp-idle-time           = 50
multi-write-group               = primary
dsa-flags               = multi-write,
no-service-while-recovering, multi-write-group-hub
trust-flags             = allow-check-password,
trust-conveyed-originator
link-flags              = ssl-encryption-remote
};
```

c. Update the DXC file:

   a. cd /opt/CA/Directory/dxserver/config/settings

   b. Edit the <hostname>-cam-tenant-router.dxc file.

   c. Remove the tenant. For example, if the tenant is cm3, locate the following line:

      set write-precedence= s010130009046-cam-tenant-cm1, s010130009046-cam-tenant-cm3, s010130009046-cam-tenant-cm4

   d. Change the entry to the following:

      set write-precedence= s010130009046-cam-tenant-cm1, s010130009046-cam-tenant-cm4;

8. Restart the dxa router on each Identity Management server.

```
su – dsa
dxserver stop all
dxserver start all
```

   Repeat steps the preceding three commands on the Provisioning Server, CA IAM CS, Policy Server, and Directory Server.

9. Remove the provisioning directory on each Provisioning Server:

   a. cd /opt/CA/Directory/dxserver/config/knowledge

   b. Edit the imps-router.dxc file and remove the tenant information

   c. For example, the file may appear as follows:

```
# CA DXserver/config/knowledge/
#
```

```
# Knowledge configuration file written by dxagent
#
# Refer to the Admin Guide for the format of the set dsa command.

set dsa "tenant-cm3-s010130009046" =
{
prefix =   <dc cm3>
dsa-name =   <dc etadb><cn tenant-cm3-s010130009046>
dsa-password            = "secret"
address         = ipv4 "s010130009046" port 20904
disp-psap               = DISP
snmp-port               = 20904
console-port            = 20905
auth-levels             = clear-password
dsp-idle-time           = 50
dsa-flags               = multi-write,
no-service-while-recovering, multi-write-group-hub
trust-flags             = allow-check-password,
trust-conveyed-originator
link-flags              = ssl-encryption-remote
};
```

10. Update the DXC file on each Provisioning Server for the Provisioning Server router:
    a. cd /opt/CA/Directory/dxserver/config/settings
    b. Edit the <hostname>-imps-router.dxc file
    c. Locate the following line:

       set write-precedence = s010130009046-impd-main, s010130009046-impd-inc, s010130009046-impd-co, s010130009046-impd-notify, tenant-cm1-s010130009046, tenant-cm3-s010130009046, tenant-cm4-s010130

    d. Replace this line with the following line:

       set write-precedence = s010130009046-impd-main, s010130009046-impd-inc, s010130009046-impd-co, s010130009046-impd-notify, tenant-cm1-s010130009046, tenant-cm4-s010130

11. Restart the DSAs on each Provisioning Server:
    a. su – dsa
    b. dxserver stop all
    c. dxserver start all
12. Stop the DSAs for tenants on all Directory servers:

    ```
    su – dsa
    dxserver stop <host name>-cam-tenant-<tenant tag>
    ```

    For example, s010130009046-cam-tenant-cm3)

    ```
    dxserver stop tenant-<tenant tag>-<host name>  stop
    ```

For example, tenant-cm17-s010130009046.

13. Remove the tenant data files from each DIR server:

```
su – dsa
cd /opt/CA/Directory/dxserver/data
ls *<tenant tag>*
```

Delete all files returned from the preceding command.

cam-tenant-<tenant tag>.ldif

tenant-<tenant tag>-<hostname>.db

tenant-<tenant tag>-<hostname>.tx

<host name>-cam-tenant-<tenant tag>-.db

<hostname-cam>--tenant-<tenant tag>-.tx

For example:

```
cam-tenant-cm3.ldif
tenant-cm3-s010130009046.db
tenant-cm3-s010130009046.tx
tenant-cm3-s010130009046.db
tenant-cm3-s010130009046.tx.
```

14. Remove knowledge files from Directory server

```
su – dsa
cd  /opt/CA/Directory/dxserver/config/knowledge
delete tenant-<tenant tag>-<hostname>.dxc
```

For example, tenant-cm3-s010130009046.dxc

Delete <host name> -cam-tenant-<tenant tag>.dxc . For example:

s010130009046-cam-tenant-cm3.dxc.

15. Remove the settings files on each directory server for the tenant:

```
su – dsa
cd /opt/CA/Directory/dxserver/config/settings
```

Delete tenant-<tenant tag>-<hostname>.dxc .For example, tenant-cm3-s010130009046.dxc)

Delete <host-name>-cam-tenant-<tenant tag>.dxc. For example, s010130009046-cam-tenant-cm3.dxc)

16. Remove the DXI file from each directory server:

cd /opt/CA/Directory/dxserver/config/servers

Remove tenant-<tenant tag>-<hostname>.dxi. For example: tenant-cm3-s010130009046.dxi

Remove <host name>-cam-tenant-<tenant tag>.dxi. For example: s010130009046-cam-tenant-cm3.dxi.

17. Remove pem files on each directory server:

su – dsa

cd /opt/CA/Directory/dxserver/config/ssld/personalities

remove <host-name>-cam-tenant-<tenant tag>.pem. For example: s010130009046-cam-tenant-cm3).pem

Remove tenant-<tenant tag>-<hostname>.pem. For example: tenant-cm11-s010130009046.pem

18. Remove auto start file on each directory server:

    su – dsa

    cd /opt/CA/Directory/dxserver/config/autostart

    Remove <host name>-cam-tenant-<tenant tag> tenant-<tenant tag>-<hostname>. For example:

    s010130009046-cam-tenant-cm3
    tenant-cm3-s010130009046

19. Remove the limits file on each directory server:

    su – dsa

    cd /opt/CA/Directory/dxserver/config/limits

    Remove <host name>-cam-tenant-<tenant tag>.dxc. For example: s010130009046-cam-tenant-cm3.dxc

    a. tenant-<tenant tag>-<host name>.dxc
       (for example, tenant-cm3-s010130009046.dxc)

20. Remove ssld files on each directory server

    a. su – dsa

    b. cd /opt/CA/Directory/dxserver/config/ssld

    c. Remove <host name>-cam-tenant-<tenant tag>.dxc. For example: s010130009046-cam-tenant-cm3.dxc)

    d. remove tenant-<tenant tag>-<hostname>.dxc. For example: tenant-cm3-s010130009046.dxc)

21. Remove the log configuration files on each directory server

    su – dsa

    cd /opt/CA/Directory/dxserver/config/logging/

    remove tenant-<tenant Name>-<DIR Server>.dxc

    remove <DIR Server>-cam-tenant-<Tenant Name>.dxc

22. Restart all DSA on all Directory machines

    a. su – dsa

    b. dxserver stop all

    c. dxserver start all

23. Verify that the DSA no longer shows via a dxserver status on each directory server:
    a. su – dsa
    b. dxserver status
    c. Verify that the dsa for the tenant are not there

       <host name>-cam-tenant-<tenant tag>. For example: s010130009046-cam-tenant-cm3

       tenant-<tenant tag>-<host name> stop. For example: tenant-cm17-s010130009046
24. Remove the Provisioning association:
    a. Use an LDAP tool such as JXplorer.
    b. Connect to your Provisioning server system using user name and password as follows:

       Use port 20391

       User DN eTDSAContainerName=DSAs,eTNamespaceName=CommonObjects,dc=etadb

       Password <your password for Provisioning DSA)

       Goto etadb –im – CommonObjects – Configuration – Parameters – Tenant Data – Tenant Identifiers

       Delete eTConfigPramValue for the tenant tag.
25. Delete the tenant from the Administrative UI

    If you support Disaster Recovery, export and import Derby. Refer to the *Disaster Recovery Guide* for steps to delete a tenant.
26. Inactivate the tenant from Arcot Admin Console as follows:
    a. Go to <host>.ca.com:9090/arcotadmin/mabamlogin.htm
    b. Search active tenants and find your tenant.
    c. Note the GUID this will help with the next step.
    d. Inactivate the tenant.
27. Delete tenant from Arcot Admin console
    a. Go to <host>.ca.com:9090/arcotadmin/mabamlogin.htm
    b. Search inactive tenants and find your tenant – the tenant was renamed by the inactive to the GUID. So you need to find the GUID which is for you tenant. If you do not have this information from the last step, look at each tenant and go to the next page and look at the DN.
    c. Delete the tenant.

Tips for redeploying a deleted tenant

- If you get a message from tenant deployment that the tenants are already registered with Provisioning Server, verify that the Provisioning Directory has been updated to remove the tenant. Return to the step 24 to remove the provisioning association.
- If tenant deployment says DSA ports are in use, make sure ports are not in use on the Directory server. See the step 23 to verify that the DSA no longer show to verify all the steps were done on the directory server. If necessary, restart the directory servers.
- If tenant deployment says AA org exists, see step 26 to delete the tenant from the Arcot Admin console.
- If tenant deployment gets errors on SMOID or duplicate records in SiteMinder, run XPSExport to find the record id and then use XPSExplorer to delete the duplicate.

Note:For high availability, you need to follow the steps for each leg, but you should only need to delete the tenant and directory from management console on the first leg.

For disaster recovery, follow the same steps at both sites, but you should only need to delete the tenant and directory from the management console at the primary site.

Reset Web Services Authentication

To ensure that users are challenged for credentials when downloading the tenant WSDL, reset the authentication.

Follow these steps:

1. Log in to the Management Console.
2. Navigate to Environment, *Tenant_Environment*, Advanced settings.
3. In Web Services, change the SiteMinder Authentication to Other, and click Save.
4. Restart the environment.
5. Select Basic Authentication again, and click Save.
6. Restart the environment.

User Synchronization

After tenant creation, you set common user synchronization parameters on the Provisioning Server. In a high-availability environment, these settings are required on one Provisioning Server node. These settings do not interrupt service or require a reboot.

Follow these steps:

1. SSH into the Provisioning Server system.
2. Log in (for example, as the root user).
3. Change the user and open the bash shell with su - imps.
4. Enable the following settings by running the following commands:

   Note: _impd_etaadmin_pwd refers to the password set in the properties.sh during the Provisioning Server kit installation.

   - Automatic Correlation (See the description following these instructions for more information on each attribute.)

     ```
     etautil -u etaadmin -p _impd_etaadmin_pwd update
     'eTConfigParamFolderName=Synchronization,eTConfigParamConta
     inerName=Parameters,eTConfigContainerName=Configuration,eTN
     amespaceName=CommonObjects' eTConfigParam
     eTConfigParamName="Automatic Correlation" to
     eTConfigParamValue=yes
     ```

   - Force single account across multiple containers

     ```
     etautil -u etaadmin -p _impd_etaadmin_pwd update
     'eTConfigParamFolderName=Synchronization,eTConfigParamConta
     inerName=Parameters,eTConfigContainerName=Configuration,eTN
     amespaceName=CommonObjects' eTConfigParam
     eTConfigParamName="Force single account across multiple
     containers" to eTConfigParamValue=ActiveDirectory
     ```

   - Use Existing Accounts

     ```
     etautil -u etaadmin -p _impd_etaadmin_pwd update
     'eTConfigParamFolderName=Synchronization,eTConfigParamConta
     inerName=Parameters,eTConfigContainerName=Configuration,eTN
     amespaceName=CommonObjects' eTConfigParam
     eTConfigParamName="Use Existing Accounts" to
     eTConfigParamValue=yes
     ```

Automatic Correlation

The automatic correlation attribute enables the alternative User Synchronization behavior whereby an attempt to update an existing, uncorrelated account triggers an automatic correlation of the account to the global user prior to the update of the account. If the parameter is No (default), the attempt to update the account will fail with a message indicating the account has not yet been correlated to this global user.

Note: This setting applies to all tenants and endpoints.

Run the following command to enable the attribute:

```
etautil -u etaadmin -p _impd_etaadmin_pwd update
'eTConfigParamFolderName=Synchronization,eTConfigParamContainerNam
e=Parameters,eTConfigContainerName=Configuration,eTNamespaceName=C
ommonObjects' eTConfigParam eTConfigParamName="Automatic
Correlation" to eTConfigParamValue=yes
```

Run the following command to read the current value of the attribute:

```
etautil -u etaadmin -p _impd_etaadmin_pwd select
'eTConfigParamFolderName=Synchronization,eTConfigParamContainerNam
e=Parameters,eTConfigContainerName=Configuration,eTNamespaceName=C
ommonObjects' eTConfigParam eTConfigParamName="Automatic
Correlation" list eTConfigParamValue
```

Run the following command to return the value to its original configuration:

```
etautil -u etaadmin -p _impd_etaadmin_pwd update
'eTConfigParamFolderName=Synchronization,eTConfigParamContainerNam
e=Parameters,eTConfigContainerName=Configuration,eTNamespaceName=C
ommonObjects' eTConfigParam eTConfigParamName="Automatic
Correlation" to eTConfigParamValue=no
```

Force single account across multiple containers

On some hierarchical endpoints, creates one account for a certain endpoint instance when a global user's account templates specify the same account name in different account containers (on same endpoint). In this case only one account is created despite the account container differences.

This behavior can be useful if the assigned account templates nominate different account containers on the same endpoint where you only want to create one account in one of these account containers.

Note: This setting applies to all tenants and Active Directory.

Run the following command to enable the attribute:

```
etautil -u etaadmin -p _impd_etaadmin_pwd update
'eTConfigParamFolderName=Synchronization,eTConfigParamContainerNam
e=Parameters,eTConfigContainerName=Configuration,eTNamespaceName=C
ommonObjects' eTConfigParam eTConfigParamName="Force single account
across multiple containers" to eTConfigParamValue=ActiveDirectory
```

Run the following command to read the current value of the attribute:

```
etautil -u etaadmin -p _impd_etaadmin_pwd select
'eTConfigParamFolderName=Synchronization,eTConfigParamContainerNam
e=Parameters,eTConfigContainerName=Configuration,eTNamespaceName=C
ommonObjects' eTConfigParam eTConfigParamName="Force single account
across multiple containers" list eTConfigParamValue
```

Run the following command to return the value to its original configuration:

```
etautil -u etaadmin -p _impd_etaadmin_pwd update
'eTConfigParamFolderName=Synchronization,eTConfigParamContainerNam
e=Parameters,eTConfigContainerName=Configuration,eTNamespaceName=C
ommonObjects' eTConfigParam eTConfigParamName="Force single account
across multiple containers" to eTConfigParamValue=""
```

Use Existing Accounts

Enable the alternative User Synchronization behavior whereby a global user's set of assigned account templates (through assigned provisioning roles) will only attempt to prescribe one account that is correlated to the global user on any particular managed endpoint. This behavior can be useful if some accounts already correlated to the global user are named differently or are in different containers than what is prescribed by the account templates included in the global user's provisioning roles and only one account is needed or allowed. If the parameter is enabled and multiple account templates for one endpoint prescribe different names and/or different containers for the account, only one account will be created.

Note: This setting applies to all tenants and endpoints.

Run the command to enable the attribute:

```
etautil -u etaadmin -p _impd_etaadmin_pwd select
'eTConfigParamFolderName=Synchronization,eTConfigParamContainerNam
e=Parameters,eTConfigContainerName=Configuration,eTNamespaceName=C
ommonObjects' eTConfigParam eTConfigParamName="Use Existing
Accounts" list eTConfigParamValue
```

Run the following command to read the current value of the attribute:

```
etautil -u etaadmin -p _impd_etaadmin_pwd update
'eTConfigParamFolderName=Synchronization,eTConfigParamContainerNam
e=Parameters,eTConfigContainerName=Configuration,eTNamespaceName=C
ommonObjects' eTConfigParam eTConfigParamName="Use Existing
Accounts" to eTConfigParamValue=yes
```

Run the following command to return the value to its original configuration:

```
etautil -u etaadmin -p _impd_etaadmin_pwd update
'eTConfigParamFolderName=Synchronization,eTConfigParamContainerNam
e=Parameters,eTConfigContainerName=Configuration,eTNamespaceName=C
ommonObjects' eTConfigParam eTConfigParamName="Use Existing
Accounts" to eTConfigParamValue=no
```

Configure Applications and Authentication Methods

After the hosting administrator deploys a tenant, you configure applications and authentication methods for the tenant environment. The tenant environment must be active before you complete this procedure.

You create an application to define how users access a software resource. For example, when you configure an application, you define what type and level of security protects the resource. If you have purchased CA CloudMinder Advanced Authentication, you can configure advanced security such as two-factor authentication to protect the resource. If you have purchased the CA CloudMinder Single Sign-on service, you can configure SSO for the application. Users only log in once to access all applications that are configured for SSO.

Once an application is configured, you can give users access to the software resource. You can configure a service that includes the application, and can assign the service to users. The users can click the icon in the User Console Home Page to access the application. For more information, see Creating a Service Using the Service Wizard (see page 115). You can also give users access to the application by making a link to the application available. For example, you can insert the link into any web page or you can send the link in an email.

Follow these steps:

1. Define the application (see page 60).
2. Choose an authentication method (see page 62).

Define the Application

You define the application details through the User Console.

Follow these steps:

1. Log in with an account that has application management privileges.

   For example, the default Tenant Administrator role has the appropriate privileges.
2. From the navigation menu, select Applications.
3. Click Applications, then Create Application.

   The Create Application screen appears.
4. Enter a name and description.

5. Associate a group with the application, if desired.

   If you specify a group on an application, use the Service wizard to create a service for the application, where there is a rule written to add\remove the requested user(s) to that group. When the service is assigned, the requested user will be a member of the group. When the service is revoked, the user will be removed from the group.

   Note: If you are configuring the application for SSO access, the group that you choose must match the group name that is indicated in the SSO partnership configuration for this application. To confirm the group name that is indicated in the partnership configuration, refer to your hosting administrator. SSO partnership configuration information is available in the CSP Console.

6. Enter a launch URL for the Application.

   A launch URL is the fully qualified domain name of the software resource you want to make available to users. For example, if a user clicks the icon for this application in the User Console Home page, they are directed to the launch URL.

   If you are configuring the application for SSO access, the launch URL is the SSO Service URL generated during SSO partnership configuration. Refer to your hosting administrator for this information.

   If you are not configuring an SSO application, simply enter the fully qualified domain name of the software resource. Use the following format:

   https://softwareresourcedomainname.com

7. Choose a logo.

   This logo is the icon for the application that appears in the User Console Home page. Users can click the icon to access the software resource.

   Note: You can also give users access to the application by inserting a link to the application into any web page.

8. Enter a welcome message.

   When users click any link you provide to the application, a login screen appears. The welcome message appears at the top of this screen.

9. Select a self-registration task.

   If a user attempts to access the application but the user does not have a CA CloudMinder account, you can allow them to self-register. Choose one of the following self-registration tasks:

   Create New Account

   Presents a simple registration form. Upon submission, creates a user account.

   Create New Account with Workflow

   Presents a simple registration form. Upon submission, forwards the user account request to one or more approvers. Creates an account upon approval.

   Create New Account with Domain Validation

   Presents a simple registration form. Upon submission, compares the email domain of the user to the tenant email domain. If they match, sends a confirmation email to the user. Creates an account upon user confirmation.

   Note: The tenant email domain is specified in the User Console, under Tenant Administration, Tenant Settings.

   Self-Registration with Attribute Exchange

   Do not choose this self-registration task in the context of application access. This task is intended for a separate purpose.

10. Choose an authentication method. (see page 126)

Choose an Authentication Method

In the Create Application screen, continue the process of creating an application by choosing one or more authentication methods. When a user attempts to access the application, the system presents a login screen. The authentication methods that you choose appear on this screen. The user can log in using their choice of the available authentication methods.

For example, you can select the Basic and Google External IDP authentication methods for an application. The application login screen displays user name and password fields for basic authentication. The login screen also displays the Google icon, so users can log in with their Google credentials.

Follow these steps:

1. In the Authentication Methods area, click Add.

   The Select Authentication Methods screen displays a list of the authentication methods available in the tenant environment.

   Note: First, create authentication methods in the system before you perform this step. You define authentication methods through the User Console, using the Authentication Methods tasks. For more information, see Create Authentication Methods.

2. Select one or more authentication methods. The following types of authentication method are available:

   Basic

   Offers simple user name and password login.

   External IDP

   Offers log in through an external credential provider, such as Google or Facebook.

   Advanced Authentication

   Offers advanced authentication methods that have been configured for your environment, such as One Time Password (OTP) authentication.

   Note: Advanced Authentication methods only appear if you have purchased the Advanced Authentication Service.

   You can choose as many authentication methods, of any type, as you want. All the methods that you select are displayed on the login page that appears when a user attempts to access the application.

3. Click Select.

   The Create Application screen appears, updated with the list of authentication methods you selected.

4. (Optional) From the drop-down list, choose a default authentication method.

   Note: Advanced Authentication methods are never available as a default.

What You Can Customize

The specific arrangement between a tenant, and one or more organizations that provide CA CloudMinder services to that tenant, governs who can customize the elements in a CA CloudMinder environment. For example, a system administrator at a service provider often performs customizations that can affect the performance of the overall environment. A tenant administrator at the tenant site can typically perform customizations that affect only their tenant environment.

The following tables define who, by default, can customize elements in an environment. However, environments can vary. See your service provider for additional details.

Customization Type		Tenant Administrators	Service Administrator	Hosting Administrator
	Customizing an Environment			
Specify logo in the User Console			Yes	Yes
	Specify Contact Us, About Us and Privacy Policy links	Yes	Yes	Yes
	Customize company name in login screens	Yes	Yes	Yes
Assign administrators		Yes	Yes	Yes
Customizing Default Tasks				
Customize the functionality and display of default tasks		Can Request	Yes	Yes
Create new tasks		Can Request	Yes	Yes
Configure options in select boxes		Can Request	Yes	Yes
Customizing Admin Roles				
Customize existing admin roles		Can Request	Yes	Yes
Create new admin roles		Can Request	Yes	Yes
Customizing Access Request Services				
Create or modify a simple service		Yes	Yes	Yes
Create or modify a complex service		Can Request	Yes	Yes
Adding Custom Business Logic				
Customize workflows		Can Request	Yes	Yes

Customization Type	Tenant Administrators	Service Administrator	Hosting Administrator
Implement custom data validation	Can Request	Yes	Yes
Implement custom business rules	Can Request	Yes	Yes

Identity Management Functionality that You Can Customize

The following table defines who can customize Identity Management functionality in an environment by default. However, environments can vary. See your service provider for additional details.

Customization Type		Tenant Administrators	Service Administrator	Hosting Administrator
Install and configure on-premise endpoints			Yes	Yes
Install and configure cloud endpoints			Yes	Yes
	Create or modify explore and correlate definitions	Can Request	Yes	Yes
	Create and modify account templates	Yes	Yes	Yes
Create and assign provisioning roles		Yes	Yes	Yes

Customizing Tenant Settings

You customize the appearance of a tenant environment to match the requirements of the customer.

Follow these steps:

1. Click Tenant Administration, Tenant Settings.
2. Supply a Title.

   It will be used on the login page and in the User Console.
3. Add an image for the logo to appear in the User Console.
4. In the Logo Link field, supply a URL for a logo to show up in the upper left corner.
5. Enter the URLs that the customer requires for the following footer links:
   - Contact Us
   - Privacy Policy
   - About Us
6. Supply the name of the tenant domain and the email address of the tenant administrator.

(Optional) Assign More Tasks to Tenant Administrators

If you decide tenant administrators should be allowed to run Explore And Correlate Definition tasks, log in to the User Console as the CSP admin. Modify the Tenant Provisioning Manager admin role and add the following tasks:

- Create Explore And Correlate Definition
- Modify Explore And Correlate Definition
- Delete Explore And Correlate Definition

Reauthentication After Password Change

Perform this procedure if you require that tenant users to re-authenticate when they change their passwords in the Change My Password task.

Follow these steps:

1. Enable ODBC Session Store Policy Servers as follows:
   a. Set the X11 DISPLAY variable.
   b. Issue the command: /opt/CA/siteminder/bin/smconsole
2. Login to Administrative UI and use the Modify Agent Configuration task.

   Select CAM-AgentObj and make sure that the FCCCompatMode is set to no.

3. Create a response *Response* in domain *tenant*Domain and create the following attribute:
   - Attribute: WebAgent-OnReject-Redirect
   - Attribute Kind: Static
   - Variable Value: /siteminderagent/forms/reauthenticate.fcc:validate
4. Create a policy *Policy* in the domain *tenant*Domain.
5. Select Add All for User Directories.
6. Add two rules in tenant_ims_realm:

```
<Rule1>:
Resource:        *task.tag=ChangeMyPassword
   Regular Expression: checked
   Action:                    Web Agent Actions, GET and POST
<Rule2>:
Resource:        *task.tag=ChangeMyPassword
   Regular Expression: checked
   Action:                    Authorization events,
OnAccessValidateIdentity
```

7. Add the response *Response* to *Rule2.*
8. Commit the creation.
9. In the Policy Server, run the command tool xpsexplorer and make the following change:
   a. Modify policy *Policy*, set ValidateIdentity to true.
   b. Restart each policy server configured for high availability.
   c. Restart the policy engine in each Secure Proxy Server configured for high availability.

2-Way SSL for Adeptra Voice Service

Follow these steps:

1. Get the external IP of the system (the IP as seen by Adeptra, not the internal IP) whitelisted by Adeptra.
2. Obtain the keystore and certificate for the test environment from CA Support.
3. Connect to the AA DB using SQLDeveloper.

   SQLPlus will not work since blob uploads are involved.
4. Obtain the certificate from Adeptra and generate the key.

   Pass the corresponding certificate to Adeptra through the person managing the partnership account.
5. Update the keystore for 2 way SSL as follows:
   a. Open the table AOK_SYSTEM_DATA.
   b. Find the row with (NAME='ws.client.keystore'), and upload the wskey.keystore file to the column VALUEBLOB.

      The keystore should be in JKS format.The key alias and password should match the value in the row with name='ws.client.keystore.pwd'
6. Update certificate for 2 way SSL
   a. Open the table AOK_SYSTEM_DATA.
   b. Change directory to the row with (NAME='adeptra.cert') and upload the Adeptra.der certificate file to the VALUEBLOB column.

      The certificate should be in binary der format.

Chapter 3: Users

This section contains the following topics:

Adding Users to CA CloudMinder

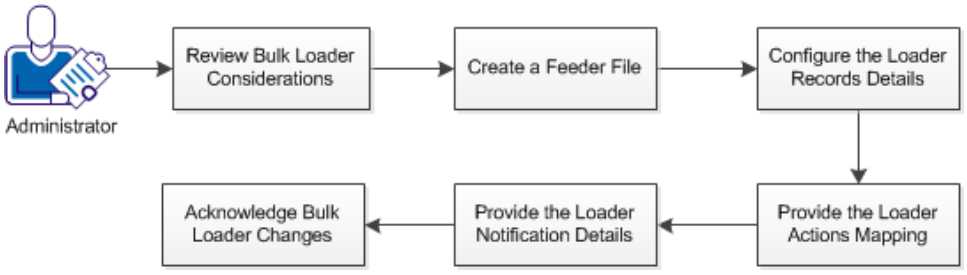
CA CloudMinder provides the following methods for adding users:

- Bulk loading multiple users
- Allowing users to self-register
- Adding a single user
- Synchronizing with an on-premise Active Directory user store

How to Add Users with a Feeder File

You can use the Bulk Loader tab to upload feeder files that are used to manipulate large numbers of managed objects simultaneously. For example, you can create 1000 users in the system manually, or you can use the Bulk Loader. The Bulk Loader task can also be mapped to a workflow process.

The Bulk Load Client is a command line utility that exists for batch processing. We recommend using the Bulk Load Client if your environment is in a cluster (for load-balancing purposes). The Bulk Load Client can be found on the Provisioning Components media.



Follow these steps:

1. Review the Bulk Loader considerations (see page 70).
2. Create a CSV or XLS feeder file (see page 72) and upload it.

3. Configure the Loader Records Details (see page 73).

   This tab allows you to specify the action and identifier fields in the feeder file.

4. Provide the Loader Actions Mapping (see page 74).

   This tab allows you to select the primary object and specify what task to execute for the action on an object.

5. Provide the Loader Notification Details (see page 75).

   This tab allows you to select users to certify Bulk Loader task changes.

6. Acknowledge and modify the progress of the Bulk Loader task changes (see page 75).

Bulk Loader Considerations

You can use the Bulk Loader tab to upload feeder files that are used to manipulate large numbers of managed objects simultaneously. Note the following considerations when using the Bulk Loader:

- Consider scheduling large bulk loads during non-peak times, such as overnight. Large bulk loads can affect performance. In some cases, a bulk load that includes many sub tasks can prevent user submitted tasks from completing until the bulk load finishes.
- If the server goes down during a long-running task, such as uploading many objects, restart the task under View Submitted Tasks. When the task restarts, it begins from the last successfully executed record.
- If you are using LDAP as a user store with Solaris, the Bulk Loader can hang during an import. To fix this issue, see the Specify LDAP Connection Settings topic in the *Configuration Guide* and apply the settings that are outlined there.
- The Bulk Loader does not set or update relationships such a group memberships, provisioning roles, and admin roles. Instead, use Policy Xpress for this purpose.
- If you use the Bulk Loader to import a large number of users, you may see out-of-memory exceptions. To address this issue, tune the following heap size memory parameters:
  - -Xmx
  - -XX:maxPermSize

    Note: For more information about tuning memory parameters, see your application server documentation.

- Using the bulk loader to manipulate many managed objects, such as creating many users, can affect performance. To improve performance, consider the following recommendations:
  - Divide one large CSV file into multiple small files when using the User Console to do bulk loads. For example, doing ten bulk loads of 10,000 users is quicker than doing one bulk load of 100,000 users.

    Note: A CSV file with more than 10,000 entries may cause issues in the system.
  - Limit the number of tasks that the user who is performing the bulk load has. For example, performance improves when the administrator who initiates the bulk load has only a few tasks. When the administrator has many tasks, Identity Management has to do more extensive permissions checks, which can affect performance.
  - Limit the number of Policy Xpress policies, which are associated with the bulk changes, that involve provisioning. Also, consider creating simple Policy Xpress policies, which do not affect performance as much as complex policies during a bulk load operation.
  - Verify that you have sufficient system resources.

Limit Data Validation to Improve Bulk Load Performance

An admin task typically includes multiple tabs. By default, bulk operations validate data on each tab in a task.

Validation can affect the performance of bulk operations. To improve performance, you can disable data validation for task tabs, if validation is not required.

Follow these steps:

1. Log in to the User Console as a user who can modify admin tasks.
2. Select Tasks, Roles and Tasks, Admin Tasks, Modify Admin Task.
3. Search for and select the task that applies in the bulk operation.
4. Select Tabs, then select the tab that you want to modify.
5. Select Do Not Validate in Bulk Operations, then click OK.
6. Repeat steps 4 and 5 for each tab that does not require data validation.
7. Click Submit.

   Data validation is disabled for the tabs that you modified.

Limit Custom Business Logic

Including custom business logic, such as business logic task handlers and event listeners, in tasks that are used in bulk operations can affect performance.

To improve performance, disable the custom business logic in bulk load operations.

Follow these steps:

1. Open the Management Console.
2. Select the applicable environment that includes the event listener or business logic task handler.
3. Select Advanced Settings, Business Logic Task Handlers (if applicable).
4. Set the value of the UseInBulkOperation property to false, then click Save.
5. Repeat step 4 for Event Listeners.
6. Once you have completed the modifications for business logic task handlers and event listeners, restart the environment.

Create a Feeder File

A Bulk Loader file is used to automate repeated actions performed on a large number of managed objects. When you upload a feeder file, the system parses and reads the feeder file.

The feeder file must have a CSV or XLS extension, and have the following properties:

- The file must contain a header line which specifies physical attributes, logical attributes, or well-known attribute names of a managed object.
- The header line must include a column that indicates the action to be performed on the records.
- Each row in the feeder file is named a record. The records contain the values for each of the attributes specified by the header line. The following options are acceptable values for an attribute:
  - Value—the attribute is set to the value you specify.
  - Value;Value;Value;...—the attribute is set to the multivalued attribute you specify.
  - ' ' (blank)—the attribute is not changed.
  - NULL—the attribute is deleted. The deletion sequence is set to NULL by default, but can be edited in the Bulk Loader File Upload Search screen.

Note: To use a hash (#) in the feeder file, enclose the hash mark in double quotes, for example, user#1 should be specified as "user#1".

Important! The feeder file must be saved with UTF-8 encoding.

Sample Feeder File for Creating Users

This sample feeder file creates users with certain required attributes.

```
action,%USER_ID%,%FIRST_NAME%,%LAST_NAME%,%FULL_NAME%,%PASSWORD%,%EMAIL%
create,JD,John,Doe,John Doe,mypassword,Johndoe@a.com
create,BD,Baby,Doe,Baby Doe,mypassword2,Babydoe@a.com
```

In the preceding code, the feeder file has the following properties:

Header

The first line of the code is the header line. The header line has physical attributes or well-known attributes for the managed object 'User'.

Action

The action column identifies the task to be performed for each record. For example, the preceding file specifies that a 'create' action should be performed on the First Name 'John'.

Sample Feeder File for Enabling Users

This sample feeder file changes the value of the |enabled| logical attribute. You specify the logical attribute in the header, and the value (in this case, true or false) in each user entry in the file.

```
action,%USER_ID%,|enable|

MODIFY,user1,false

MODIFY,user2,true
```

Loader Records Details Tab

The Loader Records Details tab displays a short preview of the records available in your feeder file. The preview table displays a maximum of 5 records. The preview table is to help users identify if they are uploading the correct file. Also, this tab allows you to identify the action you want to perform on the managed objects specified in your feeder file. You must complete the following fields:

What field represents the action to perform on the object?

Identifies the fields from the feeder file that mention the action you want to perform on the managed objects. For example, you can use a feeder file with a field 'action' that takes the values Create, Modify, and Delete. You must map each of these actions to an admin task in Loader Actions Mapping (see page 74).

What field will be used to uniquely identify the object?

Identifies the field from the feeder file that can uniquely identify the primary object.

Note: If the feeder file has an invalid header line, the feeder file records will not be displayed in the Loader Records Details tab. Select another feeder file in the case of invalid header lines. If the feeder file contains some invalid records, the detailed status of the upload will be in View Submitted Tasks under the System tab.

Loader Actions Mapping Tab

The Loader Actions Mapping tab allows you to select a primary object on which the actions specified in the feeder file will be performed. You must also map the actions from the feeder file to admin tasks for the selected primary object.

What is the Primary Object?

Identifies the primary object to be manipulated by Identity Management using the feeder file. You can select any one of the following primary objects:

- User
- Groups
- Organization

Select a task to execute for 'action'

Identifies the admin tasks to be performed for each action specified by the feeder file, such as the Delete or Modify tasks.

Note: You have to map all the actions in the feeder file to an admin task. Also, the admin tasks displayed in this field are dependent on the primary object selected. For example, if you select 'User' as the primary object, only the admin tasks related to 'User' are displayed.

Select a task for non-existing object for 'action'

Identifies the alternate admin tasks to be performed for an action specified in the feeder file in the event that the managed object does not yet exist within Identity Management, such as the Create task.

Loader Notification Details Tab

Important! By default, this tab isn't included in the Bulk Loader wizard. You must add it manually by modifying the Bulk Loader task and adding the Loader Notification Details tab. Also, this tab requires you to enable workflow in the environment.

The Loader Notification Details tab allows you to select certification managers for the Bulk Loader task. When a Bulk Loader task completes, Identity Management creates a Bulk Loader Notification for all certification managers configured for the task. This notification appears in the Home tab under Bulk Loader Notifications. Clicking on the notification displays details for tasks initiated by the bulk load operation. Certification managers can then review and acknowledge the changes detailed in the notifications.

Note: To provide a list of certification managers, use any of the available participant resolvers in the drop-down list. For more information about Participant Resolvers, see the Workflow section of this guide.

Acknowledge Bulk Loader Task Changes

The Bulk Loader Notifications contain details on all the changes that the Bulk Loader task initiated. Certification managers can review and acknowledge any changes initiated by a Bulk Loader task.

To review and acknowledge Bulk Loader task changes

1. Log in to the User Console as a user that is listed as a certification manager for a Bulk Loader task.
2. Go to Home, View my Bulk Loader Notifications.
3. Select the Bulk Loader Notification you want to review.

   The Manage Bulk Loader Notifications screen appears and displays a table listing all the Bulk Loader task changes that were initiated.

   From this screen, you can do the following:

   - To review specific task details for a create or modify object, click the hyperlink under the Description column.
   - If there are compliance violations, or if you want to remove a role that was added to a user, you can edit the user directly from the notification screen by clicking the Edit icon next to the User ID.
   - To review any roles added to a user, click the hyperlink under the Requested Role Assignments column associated with the User ID.

4. Once you have reviewed all the changes for a specific object, select the Acknowledge check box for that object.
5. Once you are done acknowledging changes, click Acknowledge to remove all selected change notifications from the list.

   Note: You can select Acknowledge All to acknowledge all of the changes in a Bulk Loader notification. This deletes the Bulk Loader Notification from the Home tab. Also, you can select the check box at the top of the Acknowledge column to select all of the change notifications on the screen at that time, and acknowledge changes screen by screen.

   When all user changes associated with a Bulk Loader task are acknowledged, the Bulk Loader Notification disappears from the Home tab.

Configure Email Notifications for Bulk Loader Tasks

In some environments, bulk operation email notifications are configured by default. To check if bulk operation email notifications are configured in your system, go to System, Email, View Email, and search on the term 'bulk'.

If no email notifications are configured in your environment, configure the email that is sent when a bulk operation completes.

Follow these steps:

1. Navigate to System, Email, Create Email in the User Console.
2. Complete the required fields on the Profile tab.
3. On the When to Send tab, complete the following steps:
   a. Select Task Completes in the first field.
   b. Select Bulk Loader in the second field.
4. Complete the Recipients and Content tabs, then click Submit.

   Email notifications are configured for bulk loader tasks.

Schedule a Bulk Loader Task

The Bulk Loader task can be scheduled in the system. To schedule the Bulk Loader task, add a Scheduler tab to the task.

Modify the Parser File for the Bulk Loader

To modify the parser used to parse feeder files, configure the corresponding admin task.

To modify the Bulk Loader admin task

1. Navigate to Roles and Tasks, Admin Tasks, Manage Admin Task.
2. Search for the Bulk Loader task.

3. Select the Bulk Loader task, and click Select.
4. Select the Search tab for the Bulk Loader task.
5. Click Browse to locate search screens.

   The list of available search screens is displayed.
6. Select a Search screen and click Edit.

   The Search screen details appear.
7. (Optional) Edit the Parser Fully Qualified Name.

   The Parser Fully Qualified Name must match the name of your parser file.

   Note: For more information about creating a custom CSV parser, see the Javadoc for the FeederParser class. If you use JBoss as your application server and you create a custom parser, the custom parser file must be in the iam_im.ear/user_console_war/WEB-INF/classes directory.
8. Click OK.

Web Service Support for the Bulk Loader

The Bulk Loader has a web service API that can be called using the Identity Management Task Execution Web Service (TEWS) interface. TEWS allows client applications to submit remote tasks to Identity Management for execution. This interface implements the WSDL and SOAP open standards to provide remote access to Identity Management.

Identity Management includes Java client samples that demonstrate calling the Bulk Loader as a web service. The Java samples are located in the following source file:

admin_tools\samples\WebService\Axis\optional\ObjectsFeeder.java

Data samples and documentation for calling the Bulk Loader as a web service are located in the following directory:

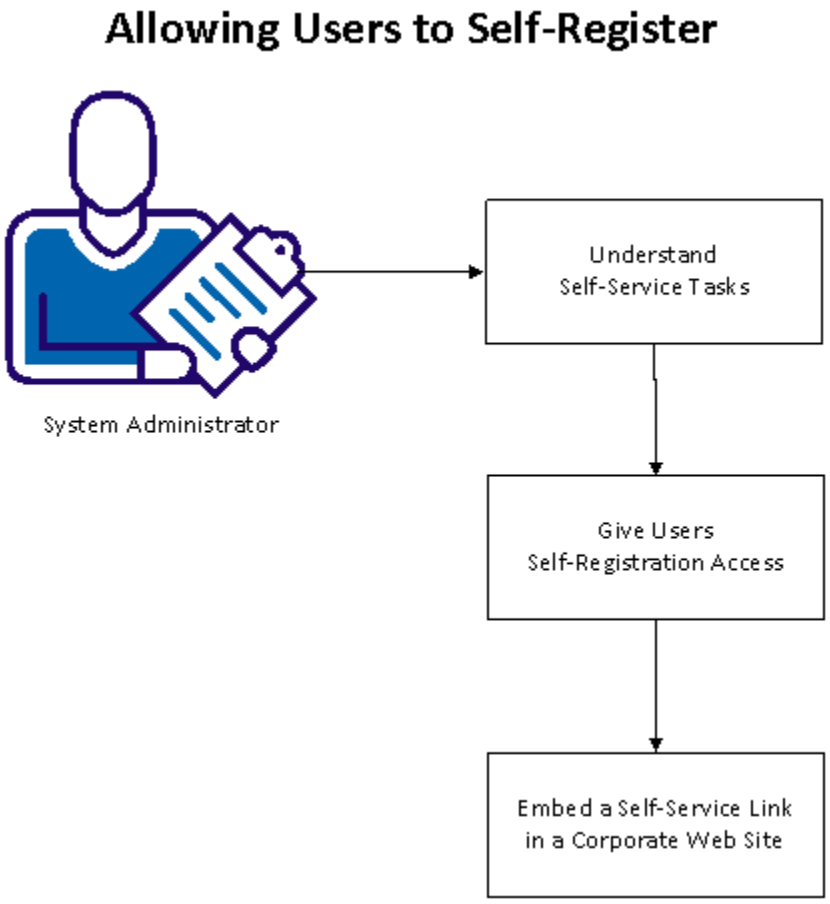
admin_tools\samples\Feeder\

Note: For more information, see the *Programming Guide for Java*.

Allowing Users to Self-Register

Self-service tasks allow users to manage their own environment. The Self-Registration task allows users to create their own user account and profile from a publicly available User Console. For example, Bentley Cola allows new employees and customers to create their own user accounts and profiles through a link embedded in the Bentley Cola corporate web site.

The following diagram shows the information to understand, and the steps to perform, in allowing users to self-register.



The following topics provide details on how to grant users self-registration access.

1. Understand Self-Service Tasks (see page 79).
2. Give Users Self-Registration Access (see page 79).
3. Embed a Self-Service Link in a Corporate Web Site (see page 80).

Self-Service Tasks

Self-service tasks are actions that users can take, typically through the User Console, to manage their own profiles. User accounts are configured by default to grant the user access to certain self-service tasks, such as changing their password and profile information. A system administrator with appropriate privileges can modify which self-service tasks are granted to a user by default.

Self-service tasks are divided into two types:

- Public tasks--Tasks that users can access without providing login credentials. Examples of public tasks are self-registration, forgotten password, and forgotten user ID tasks.
- Protected tasks--Tasks for which users provide valid credentials. Examples include tasks for changing passwords or profile information.

The following table lists the default self-service tasks.

Task Type	Tasks
Public Task	■ Self-registration ■ Self-registration with email confirmation ■ Forgotten Password Reset ■ Forgotten User ID
Protected Task	■ Request & View Access--Allows users to request access to, and remove, services. ■ Change My Password ■ Modify My Profile

Access Self Service Tasks

Once you have configured the self-service tasks for your environment, you can add URLs for these tasks to a corporate website.

URLs for self-service tasks have the following format:

https://*domain*/iam/im/*public_alias*/ui7/index.jsp?task.tag=*task_tag*

where:

- *domain* is the fully qualified domain name of the web server in the environment where CA CloudMinder is running.
- *public_alias* is the public alias of the environment. The system administrator defines the public alias when the environment is created.
- *task_tag* is the unique identifier for the task.

  For the default Forgotten Password Reset task, the task tag is ForgottenPasswordReset.

  https://*domain*/iam/im/*public_alias*/ui7/index.jsp?task.tag=ForgottenPasswordReset

  For the default Forgotten User ID task, the task tag is ForgottenUserID:

  https://*domain*/iam/im/*public_alias*/ui7/index.jsp?task.tag=ForgottenUserID

Embed a Self-Service Link in a Corporate Web Site

To allow access to a public self-service task from a corporate website, you can add a link to any web page. When a user clicks the link, a task screen opens. When the user completes the task, they are redirected to the User Console by default.

To change the page to which users are redirected, you can append the task.RedirectURL tag to the URL associated with the link as follows:

<A href="https://*domain*/iam/im/*public_alias*/ui7/index.jsp?task.tag=*tasktag*&task.RedirectURL=http://*domain*/*redirect_URL*">*link text*</A>

domain

The fully qualified domain name of the web server in the environment where CA CloudMinder is running.

public_alias

A unique string that is added to the URL for access to public tasks.

Public tasks are self-service tasks, such as self-registration or forgotten password tasks. Users do not need to log in to access public tasks.

tasktag

The unique identifier for the task. To determine the task tag, use Modify Admin Task to view the profile for the task.

redirect_URL

The URL to which users are directed after they submit the task.

For example, you can redirect users to a Welcome page after they self-register.

link text

The text that users click to access the target URL.

For example, a company can add a link that allows users to reset a forgotten password and then directs them to a welcome page.

The following HTML represents an example of link text:

<A href="https://myserver.mycompany.org/iam/im/Employees/ui7/index.jsp?task.tag=ForgottenPasswordReset&task.RedirectURL=http://myserver.mycompany.org/ welcome.html">Reset My Password</A>

To return users to the page where they accessed the self-service task, specify RefererURL as the value of the task.RedirectURL tag as follows:

<A href="https://*domain*/iam/im/*public_alias*/ui7/index.jsp?task.tag=*tasktag*&task.RedirectURL=RefererURL</A>

Self-Registration with Email Confirmation

To increase security, the Create New Account self-registration task sends an email to users when they register. The email requires users to confirm their registration and validate their email address by clicking a link to complete the registration process.

The self-registration task also includes the following additional security features:

- **Password meter**

  Indicates how secure a self-registered user password is.

  The user enters a password and immediately sees one of the following password levels displayed on screen:

  Very Weak

  Weak

  Better

  Medium

  Strong

  Strongest

- **Captcha support**

  Self-registration can use Google reCaptcha to prevent malicious attacks from automated "bots." When you add the Captcha control to a self registration task, users prove that they are not screen reader programs by typing distorted words or numbers into a verification field.

  The following screen shows the Captcha control.

Important! In its default configuration, self-registration uses the reCaptcha service from Google, to discourage abuse of self-registration by automated bots. We cannot guarantee that Google will continue to provide the reCaptcha service in its current form; changes by Google may result in self-registration becoming nonfunctional. You can reconfigure self-registration to function without reCaptcha.

Administrators complete the following high level steps to configure self-registration with email confirmation:

1. Configure a required attribute in the user store (see page 83).
2. Configure the self-registration task (see page 84), including the password meter and Captcha support.
3. Configure the self-registration confirmation task (see page 87).
4. Configure the email (see page 88).
5. Associate the self-registration task with the tenant environment (see page 89).

Configure Required Attribute

The user store must include the following well-known attribute to support self-registration with email confirmation:

- %ACTIVATION_ID%—Identifies the attribute that stores a randomly generated activation number. The activation number and user ID are included in the link that users click to complete the registration process.

You map the %ACTIVATION_ID% well-known attribute to an available user store attribute in the directory configuration file (directory.xml). If there is no available attribute, extend the user store schema. For more information about extending the schema, see the documentation for your user store.

Configure a Custom Self-Registration Task

The product includes the following predefined self-registration tasks:

Task	Tag	Description
Create New Account	CAMSelfRegistration	Supports self-registration with email confirmation
Create New Account	CAMSelfRegistrationDomainValidation	Supports self-registration with email confirmation and validates the email domain
Create New Account	CAMSelfRegistrationWorkflow	Supports self-registration with email confirmation, and includes a one-step workflow approval process.

To enable self-registration with email confirmation, these tasks are associated with a business logic task handler (BLTH), which performs custom business logic during data validation operations for a current task.

The BLTHSelfRegEmailConfirm business logic task handler performs the following operations when the user self registers:

- Adds a registration code to a well-known attribute on the user.

  The registration code is stored on the user object in a well-known attribute. You specify the well-known attribute when you configure the self-registration task.

- Displays an on-screen message that instructs users to complete the registration process as described in email.

The default self-registration tasks also includes a password meter and a Captcha control.

If the default tasks do not meet business requirements, administrators can create a custom task.

Follow these steps:

1. Make a copy or edit an existing self-registration task.
2. Add the BLTH that enables email confirmation by completing the following steps:
   a. Click Business Logic Task Handlers, Add.
   b. Enter the following values:
      - Name: BLTHSelfRegEmailConfirm
      - Java Class: com.netegrity.webapp.selfreg.BLTHSelfRegEmailConfirm
   c. (Optional) Add properties to the BLTH.

      Two properties are supported:

      WellKnown

      Specifies the well-known attribute that BLTHSelfRegEmailConfirm uses to store the activation code.

      If you do not specify a value, the default %ACTIVATION_ID% well-known attribute is used.

      Message

      Specifies an optional message that overrides the default message.

      The default message, which resembles the following, appears in the User Console when the user submits the self-registration task:

      "Your account has been created. Please check your email and follow the directions to enable your account."
   d. Click OK twice to return to the Profile tab.
3. Configure the task screen:
   a. Click Tabs.
   b. Browse for the CAM Self Registration Profile screen. Select the screen, then click Edit.
   c. To enable configure the password meter, click the pencil icon to edit the Choose a Password field.
   d. To configure Captcha settings, including the display theme,edit the Captcha field.

      If the Captcha field is not defined for the self-registration profile screen, add a separator field. Select Captcha as the style.

Enter the following required values in the Captcha field definition:

- PrivateKey: 6Lduf78SAAAAAOjrYFefpGfu9gGII5lGxy-RIGCq
- PublicKey: 6Lduf78SAAAAADgXIU0vLq4lrFWH96Rc5zac730f

e. Make other screen changes as needed.

f. Click OK to return to the Select Screen Definition screen. Click Select.

4. Click OK, then Submit.

Configure the Self-Registration Confirmation Task

Configure the task that users are redirected to when they click the link in the registration confirmation email.

Follow these steps:

1. Select Tasks, Roles and Tasks, Admin Tasks, Manage Admin Tasks, Create Admin Task.
2. Select Create a new admin task.
3. On the Profile tab, complete the required fields:
   - **Name**: CAM Self Registration Email Confirm
   - **Tag**: SelfRegistrationConfirm

     Note: The task name is required when you create the self-registration email.
   - **Category**: SelfReg
   - **Primary object**: User
   - **Action**: Modify
   - **Public task:** Select the check box.
4. On the Search tab, select the SelfRegEmailConfirm search screen.

   Note the following guidelines when selecting the search screen:
   - If the SelfRegEmailConfirm screen is not available in the list of screen definitions, add it by clicking New and selecting Self Registration Email Confirm User Search.

     If you create a new search, select a well-known attribute to store the activation code used in the email link. The well-known attribute must match the well-known attribute that you specified when you configured the BLTH (see page 84) for the self-registration task.
   - If you copied the task from another task, make sure that no tabs are associated with the task.
5. On the Tabs tab, add the ActivateUser tab.
6. Click submit to save the task.

Configure the Confirmation Email

The confirmation email includes a self-registration link that the user click or copy to a browser to complete the registration process.

Follow these steps:

1. Select System, Email, Create Email, Create a new object of type Managed Email.
2. Complete the tabs by providing the following input:
   - **Profile tab**

     Specify a name and category for the email. Select the Enabled check box.
   - **When to Send tab**

     In the first list box, select Task Completes.

     In the second list box, select the self registration task that you created (see page 84).

     The self-registration task should be associated with the BLTHSelfRegEmailConfirm business logic task handler.
   - **Recipients tab**

     Select User.

     You can select additional user types, if other users should receive the email.
   - **Content tab**

     Specify the message that self-registered users see in the confirmation email.

     Include a link to the self-registration confirmation task.

     For example:

     ```
     <p>To complete the registration process and validate your email
     address, click on the following link:</p>
     <p>https://server/iam/im/environment_public/ui7/index.jsp?t
     ask.tag=SelfRegistrationConfirm&amp;userid={'Attribute:
     %USER_ID%'}&amp;v={'Attribute: %EMPLOYEE_NUMBER%'}</p>
     ```

     In this example:

     server

     Specifies the server for your environment

     SelfRegistrationConfirm

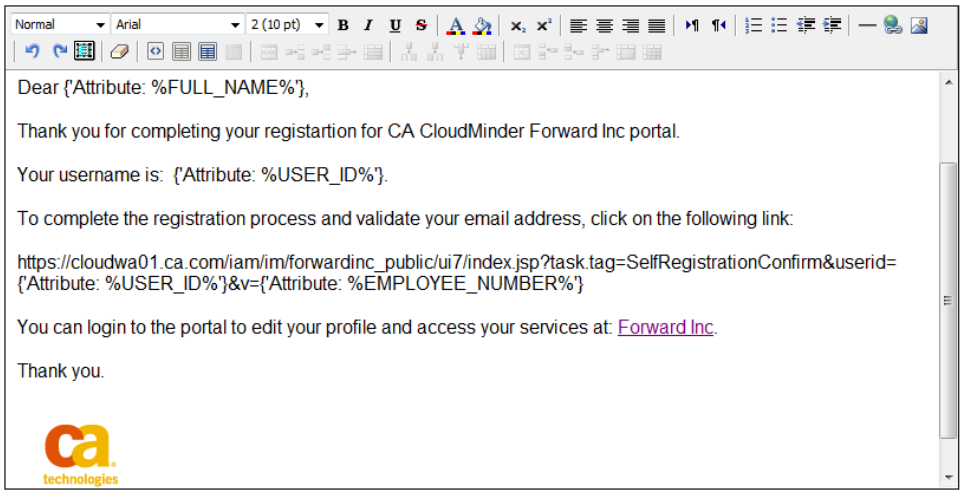
     Specifies the self registration confirmation task that you created.

     v

     Specifies the well known attribute that stores the validation code. In this example its %EMPLOYEE_NUMBER%

Note: To avoid issues when specifying the link and well-known attributes, create the email in HTML mode. To use HTML mode, click the <> icon in the email editor.

The following screen shows a sample confirmation registration.



Associate the Self-Registration Task with the Tenant Application

After you configure self-registration with email confirmation, you can associate the self-registration task with a tenant environment.

Follow these steps:

1. Open Applications, Modify Application.
2. Search for and select the tenant application.
3. Select the self-registration task.
4. Click Submit.

Creating and Configuring a User

User profiles allow administrators to manage user information; manage privilege, application, and service access; and grant users self-management for their own accounts and services. Creating user profiles is a common task for a system administrator.

When creating and configuring a user, consider the following user account elements:

Self-Service Tasks: User profiles are configured by default to grant the user access to certain self-service tasks, such as changing their password and profile information. A system administrator with appropriate tasks can modify which self-service tasks are granted to a user by default.

Groups: Groups simplify role management. For example, a system administrator with appropriate tasks can configure multiple roles for the system to assign automatically to a user who is added as a member of a group.

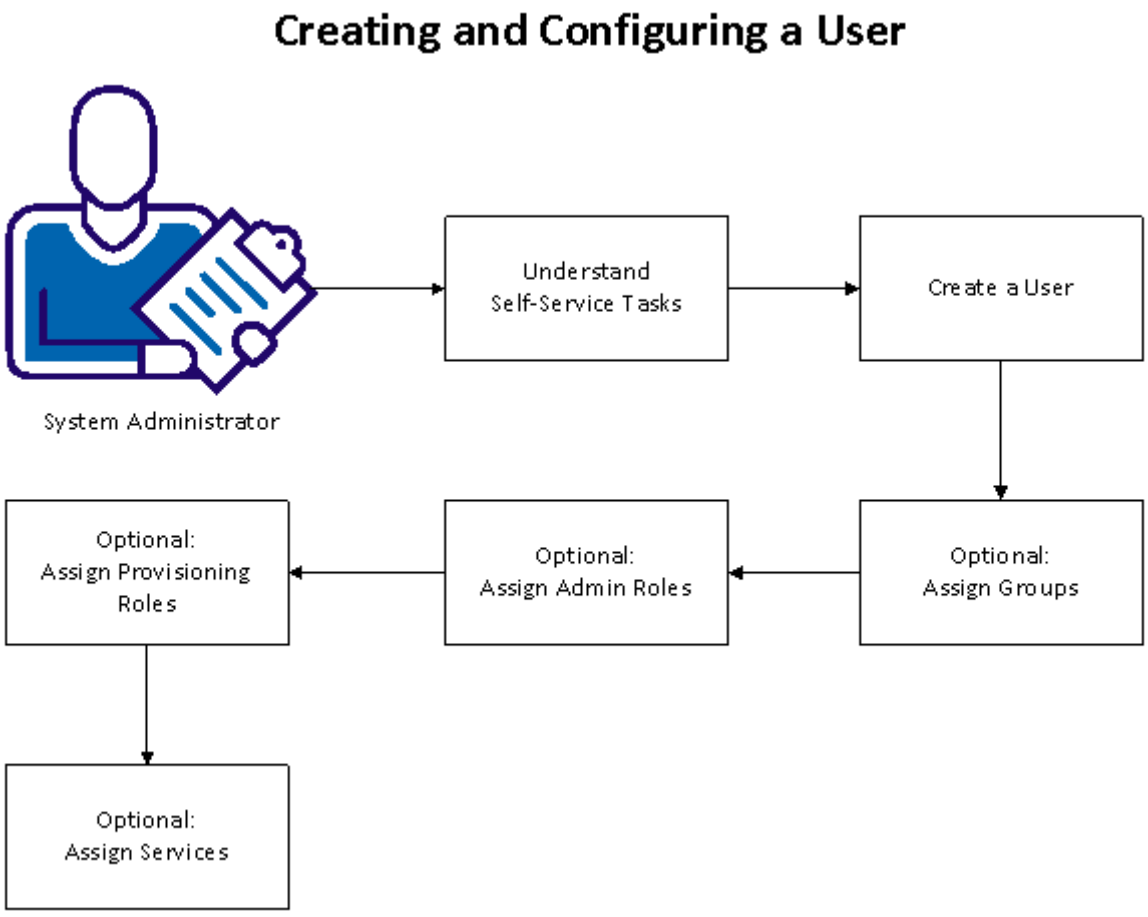
Admin Roles: Admin roles define the tasks that a user can perform in the User Console. For example, a task can allow a user to modify user account information, such as the address or job title. Another task can allow a user to administer tasks, such as granting a user membership in a group. When you assign an admin role to a user, the user can perform the tasks associated with the role.

Endpoint Accounts and Provisioning Roles: Accounts that exist on other systems are named Endpoints Accounts. You can assign accounts in endpoints to CA CloudMinder users through provisioning roles. For example, a user needs an Exchange account for email, an Oracle account for database access, and an Active Directory account to use a Windows system. When you assign a provisioning role to a user, the user receives the endpoint accounts the provisioning role specifies.

Services: Services allow you to combine you choice of user tasks, roles, groups, and attributes into a single package. You can manage this package of privileges as a set. For example, all new Sales employees need access to a defined set of tasks, accounts on specific endpoint systems, and information added to their user account profiles. When you assign a service to a user, the user receives the entire set of roles, tasks, groups and account attributes the service specifies.

Password Policies: Password policies manage user passwords by enforcing rules and restrictions governing password expiration, composition, and usage. If a system administrator has created password policies for your environment, those policies are applied automatically to new users matching one or more password policies rules. A system administrator with appropriate tasks can modify password policies.

The following diagram shows the information to understand, and the steps to perform, in creating and configuring a user.



The following topics explain creating users in depth, and how to configure them.

1. Understand Self-Service Tasks (see page 92)
2. Create a User (see page 92).
3. Assign Groups (see page 93).(if needed)
4. Assign an Admin Role (see page 94). (if needed)
5. Assign a Provisioning Role (see page 94). (if needed)
6. Assign Services (see page 95). (if needed)

Self-Service Tasks

Self-service tasks are actions that users can take, typically through the User Console, to manage their own profiles. User accounts are configured by default to grant the user access to certain self-service tasks, such as changing their password and profile information. A system administrator with appropriate privileges can modify which self-service tasks are granted to a user by default.

Self-service tasks are divided into two types:

- Public tasks--Tasks that users can access without providing login credentials. Examples of public tasks are self-registration, forgotten password, and forgotten user ID tasks.
- Protected tasks--Tasks for which users provide valid credentials. Examples include tasks for changing passwords or profile information.

The following table lists the default self-service tasks.

Task Type	Tasks
Public Task	■ Self-registration ■ Self-registration with email confirmation ■ Forgotten Password Reset ■ Forgotten User ID
Protected Task	■ Request & View Access--Allows users to request access to, and remove, services. ■ Change My Password ■ Modify My Profile

Create a User

Use this procedure to create a user profile. Depending on how the Create User task is configured, you can also use this task to define additional profile elements. You can add a user to a group, or can make the user a member of an admin or provisioning role.

Follow these steps:

1. Log in to the User Console as a user with user management tasks.

   The default User Manager role grants the appropriate tasks.

2. Select Users, Manage Users.
3. Select Create User or Create User with Generated Password.

   The difference between these tasks is the Create User task includes a password field. The Create User with Generated Password sends an email to the new user that requires that user to set a password.

4. Complete the fields for the user profile information, as needed.
5. Click Next.
6. Complete the fields on the other tabs in the task, if applicable.

   For example, add the user to a group, or assign an admin role, provisioning role, or service to the user, if these options are available.
7. Click Finish.

   The user is created.

If the Create User task is not configured to allow you to add groups, roles or services for the user, first create the user, then use the following procedures to complete user configuration:

Assign Groups (see page 93)

Assign Admin Roles (see page 94)

Assign Provisioning Roles (see page 94)

Assign a Group to a User

You can make a user a member of a group.

Follow these steps:

1. Log in to the User Console as a user with user management tasks.
2. Select Tasks, Groups, Modify Group Members.

   A list of the groups you can manage appears.
3. Select a group and click Select.

   The list of users that are assigned to the group appears.
4. Click Add a user.
5. Search for a user to whom you want to assign the group.

   To display a list of all users for whom you have administrative privileges, click Search without modifying the search criteria.
6. Select a user and click Select.

   An updated list of users that are assigned to the group appears.
7. Click Submit.

   The specified user becomes a member of the group.

Assign an Admin Role to a User

You can assign admin roles to an individual user.

Follow these steps:

1. Log in to the User Console as a user with user management tasks.

   Note: The default User Manager role grants the appropriate tasks.

2. Select Users, Manage Users, Modify User.

   A search screen appears.

3. Search for a user to whom you want to assign the new role.

   To display a list of all users for whom you have administrative tasks, click Search without modifying the search criteria.

4. Select a user and click Select.

   The user profile appears.

5. Select the Admin Roles tab.

6. You can add an admin role from a list of available roles. You can also copy the role from a user that already has the desired role. Choose one of the following options:

   - Click Add an admin role, and search for the role you want to assign. A role only appears in the list of search results if you are an administrator of the role. Select the desired role and click Select.
   - Click Copy from a user, and search for a user that already has the desired role. Select the user, then select the desired role and click OK.

   An updated list of roles that are assigned to the user appears.

7. Click Submit.

   The user receives the specified roles.

Assign a Provisioning Role to a User

You can assign provisioning roles to an individual user.

Follow these steps:

1. Log in to the User Console as a user with the Modify Provisioning Role Members/Administrators task.
2. Select Roles and Tasks, Provisioning Roles, Modify Provisioning Role Members/Administrators.

A search screen appears.

3. Select the role you intend to assign to the user.

   The Membership tab appears.

4. Click Add User.

5. Search for a user to whom you want to assign the role.

   To display a list of all users for whom you have administrative tasks, click Search without modifying the search criteria.

6. Select a user and click Select.

7. Select the Provisioning Roles tab.

8. Click Add a provisioning role, and search for the role you want to assign. A role only appears in the list of search results if you are an administrator of the role. Select the desired role and click Select.

   An updated list of roles that are assigned to the user appears.

9. Click Submit.

   The specified roles are assigned to the user.

Assign a Service to a User

You can assign a service directly to an individual user. This user becomes a *member* of the service.

Follow these steps:

1. Navigate to Services, Request & View Access.

   A list of services you can administer appears.

2. Select the service that you want to assign to a user and click Select.

   A list of users that are assigned to the service appears.

3. Click Request Access.

4. Search for a user to whom you want to assign the service.

   To display a list of all users for whom you have administrative privileges, click Search without modifying the search criteria.

5. Select a user and click Select.

   An updated list of users that are assigned to the service appears.

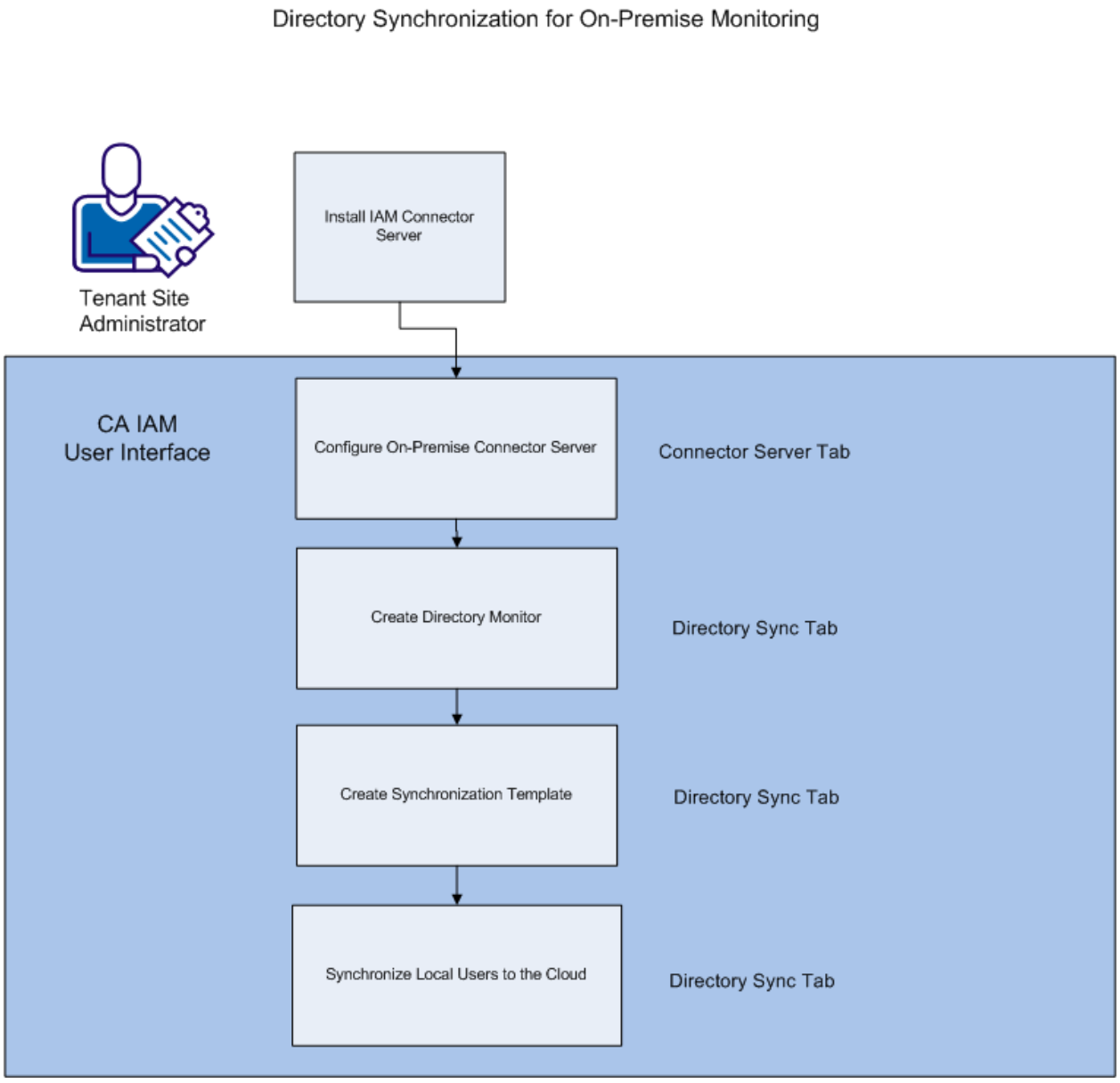
6. Click Save Changes.

   The user receives the specified service. The user receives all applications, roles, groups, and attributes you included in the service.

Directory Synchronization for On-Premise Monitoring

As a tenant Site Administrator who wishes to use directory synchronization to populate a cloud-based environment with on-premise user details, follow this process:

1. Receive the username, password, URL, and tenant name for the cloud-based CA IAM CS from the CA CloudMinder System Administrator for your environment. This information allows you to connect your local CA IAM CS to the cloud for synchronization.
2. Download and install CA IAM CS in your on-premise environment. The installation package is available from support.ca.com.
3. Configure an on-premise Connector Server to connect to the preconfigured cloud-based CA IAM CS.
4. Create a directory monitor. Monitors capture changes that you make locally, and report them for synchronization.
5. Create a Synchronization template to locate on-premise users.
6. Update tenants to use the correct value for User Type.
7. Synchronize users from your local store to the cloud. When you finish this step, CA IAM CS automatically syncs any future changes in your ADS users with the cloud store.


Directory Synchronization for On-Premise Monitoring
Tenant Site Administrator
Install IAM Connector Server
CA IAM User Interface
Configure On-Premise Connector Server
Connector Server Tab
Create Directory Monitor
Directory Sync Tab
Create Synchronization Template
Directory Sync Tab
Synchronize Local Users to the Cloud
Directory Sync Tab

Install CA IAM CS

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 a 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://*cloudcs_hostname*:22002. 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 sync issue.
7. On the Port Configuration screen, accept the default values.
8. Enter HTTP Proxy credentials if your environment uses an HTTP proxy.

9. Select the Enable DirSync checkbox on the DirSync screen. If you do not select it, you will be unable to complete the synchronization process.
10. Complete the wizard. You can install multiple connector servers in your environment, depending on your needs.

Create a Connector Server Entry

You can create an on-premise Connector Server entry to connect to the cloud-based CA IAM CS. Your System Administrator preconfigures the cloud CA IAM CS.

Follow these steps:

1. Log in to the on-premise CA IAM CS.
2. Select the Connector Servers tab, and click Add at the top of the Connector Server Management pane.
3. In the Add Connector Server dialog, select Cloud Server, and enter the credentials that the System Administrator provided. The credentials include the username, password, URL, and tenant name.
4. Click OK to save the entry.

   Ensure that the newly-created Cloud-based CA IAM CS appears in the list. If it does not, contact your System Administrator.

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 Synchronization Template

Synchronization templates control how local changes are propagated to your endpoints, and how they are formatted. You can create a synchronization template to connect your local user store with the cloud.

Follow these steps:

1. Log in to CA IAM CS, and select the Directory Sync tab.
2. 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. Enter a name, select Cloud Server from the server type pull-down menu, and the endpoint type you want from the Endpoint Type pull-down menu.
4. Click the Browse button and navigate to the account container where your synchronized accounts are stored, if needed.
5. Select the User Store tab,
   a. Select the LDAP URI for the user store you want to synchronize in the Monitor Source area.
   b. Click Browse to locate container details in the Trigger Container area,

      or
   c. Add a Trigger group:
      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, and click Search.

         A list of available Active Directory groups appears.
      c. Select the group or groups you want using the shuttle control, and click OK.
   d. To enter an optional filter statement in the User inclusion filter area, click the Filter checkbox.
6. Select the Attributes tab to configure how the template maps Active Directory source information to the target endpoint:
   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 multivalued 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.

d. To set additional synchronization preferences, select the Options tab, and select one or more of the following settings:

Suspend Deleted Accounts

Suspends cloud-based accounts when the corresponding ADS user is deleted.

Send Modifications as Deltas:

Sends only modified user attributes during a synchronization, not all user attributes.

One Level:

Synchronizes only ADS users in the parent Trigger Container. Users in child containers are ignored.

Send Renames as Delete/Add:

Synchronizes changed 'User ID' attributes by deleting the older entry and replacing it with the new information. For example, if you change from sAMAccountName to uid, synchronization deletes the cloud-based accounts and recreates them with new User ID values, rather than renaming them.

7. Click OK.

Synchronize Users

When you have created a directory synchronization template, you can synchronize your local user store to the cloud-based CA IAM CS.

Click the Synchronize button in the template area of the Directory Sync tab. An on-premise user that does not exist in the cloud environment is created according to the attribute mapping. Once you have synchronized your users, CA IAM CS automatically mirrors any future changes in your ADS users to the cloud store.

Deleted Active Directory Account Not Reflected in CA CloudMinder

Symptom:

After configuring directory synchronization with an Active Directory user store, deleting an account in Active Directory does not delete the corresponding CA CloudMinder account.

Adding or updating user information in Active Directory does update CA CloudMinder successfully.

Solution:

By default, the Active Directory mail attribute, searchFlags, is set to 0x00000001. This setting allows the mail attribute to be indexed for Active Directory searches but it prevents Active Directory from saving it in a tombstone object.

To enable account deletion in CA CloudMinder, use the AdFind or AdMod commands to set the third bit number of the search flag to a 1 (0x00001001). Setting the third number to 1 enables the attribute to be saved in the tombstone object. Once mail is saved in the tombstone object, it is included in the change notification that Active Directory sends to the on-premise CA IAM CS.

Validate Email During User Creation

You can determine whether users can enter an email address that already exists in the system. By default, the product allows multiple users to have the same email address.

You can enable a validation step that prevents users from entering an email address that already exists in the system.

Follow these steps:

1. In the Management Console, select Environments, *Tenant Environment*.

   The Management Console URL resembles the following address:

   http://hostname:port/iam/immanage
2. Select Advanced Settings, Business Logic Task Handlers.
3. Add a User defined property named checkDuplicateEmail. Set the value to true to prevent duplicate email addresses.
4. Save the settings and restart the environment.

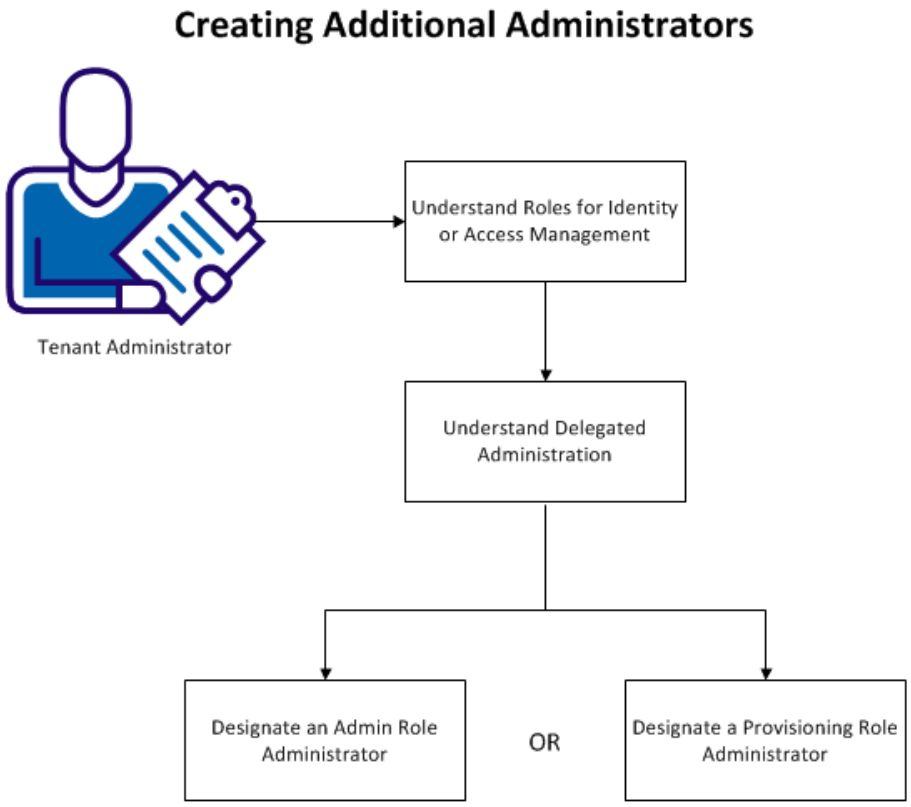
Creating Additional Administrators

Typically, a system or tenant administrator creates additional administrators. The following instructions use a tenant administrator as the example user.

As a tenant administrator, you can give users roles. Each role allows a user certain privileges, such as the ability to use a task in the User Console or an account in an endpoint.

You can be solely responsible for granting all roles to users in your system. You can also share the work of granting user roles by designating additional administrators. This approach is named *delegated administration*.

The following diagram shows the information to understand, and the steps to perform, in creating additional administrators.



The following topics explain how to create additional administrators:

1. Understand Roles for Identity or Access Management (see page 105).
2. Understand Delegated Administration (see page 105).
3. Designate an Admin Role Administrator (see page 106).

   OR

4. Designate a Provisioning Role Administrator (see page 107).

Roles for Identity or Access Management

To enable management of user identities and their access to other accounts, CA CloudMinder provides two types of roles. With an admin role, a user can manage users, such as modifying a user password or group membership. Admin roles can also include any task that appears in the User Console. With a provisioning role, a user has access to other business applications, such as an email system.

Further details about roles are outlined in the following table:

Type of Role	Purpose
Admin role	Contains admin tasks that, when granted that role, a user can perform in CA CloudMinder, such as tasks for managing users.
Provisioning role	Contains account templates that define accounts that exist in managed endpoints, such as an email system. The account templates also define how user attributes are mapped to these accounts.

Delegated Administration

Delegated administration is the use of roles to share the work of managing users and granting application access.

For each role in the system, a user can serve one or more of the following functions:

Function	Definition
Role Owner	Modifies the role.
Role Administrator	Assigns the role to users and other role administrators.
Role Member	Uses the role to perform admin tasks or use an endpoint account.

By dividing these functions between users, you can share the work of managing a role. For example, you can have lower-level administrators manage role membership and higher-level administrators modify the role.

You can implement delegated administration in the following ways:

- Directly designate a user as an administrator for a given role.
- Configure *admin rules* for a role. Admin rules define which users can be administrators of a role. The system automatically creates additional administrators when users meet the criteria specified in the rules.

  Note: Only an administrator with privileges to modify a role can configure admin rules for that role. Typically, system administrators perform this activity. To configure admin rules that automatically delegate administration for a role, see the section entitled Admin Roles in the Reference Information section of the Online Help.

Designate an Admin Role Administrator

You can designate a user as an administrator of an admin role. The administrator can then assign the role to other users, granting them access to the tasks associated with the role.

Follow these steps:

1. Log in to the User Console as a user who can modify admin role administrators.
2. (Optional) To confirm the association between a task and an admin role, navigate to Roles and Tasks, then do one of the following actions:
   - Click Admin Roles, View Admin Role. Select the role for which you want to add an administrator, then click the Tasks tab to view a list of tasks that are associated with the role.
   - Click Admin Tasks, View Admin Tasks. Select a task that you want an administrator to be able to grant to other users, then click the Role Use tab to view a list of roles that are associated with the task.
3. From the navigation menu, select Roles and Tasks, Admin Roles, Modify Admin Role Administrators.

   A list of the admin roles you can administer appears.
4. Select the role for which you want to add an administrator and click Select.

   A list of current role administrators appears.
5. Click Add a User.

   A search screen appears.

6. Search for the user you want to add as an administrator and click Select.

   An updated list of role administrators appears.

7. Click Submit.

   The user becomes an administrator of the role. This step completes the process of delegating administration of an admin role. The administrator can now assign the role to other users, granting access to the associated tasks.

Designate a Provisioning Role Administrator

You can designate a user as an administrator of a provisioning role. The administrator can then assign the role to other users, granting them access to the endpoints accounts associated with the role.

Follow these steps:

1. Log in to the User Console as a user with role management tasks.
2. From the navigation menu, select Roles and Tasks, Provisioning Roles, Modify Provisioning Role Members/Administrators.

   A list of the provisioning roles you can administer appears.

3. Select the role for which you want to add an administrator and click Select.
4. Click the Administrators tab.

   A list of current role administrators appears.

5. Click Add a User.

   A search screen appears.

6. Search for the user you want to add as an administrator and click Select.

   An updated list of role administrators appears.

7. Click Submit.

   The user becomes an administrator of the role. This step completes the process of delegating administration of a provisioning role. The administrator can now assign the role to other users, granting access to the associated endpoint accounts.

Chapter 4: Assigning Roles

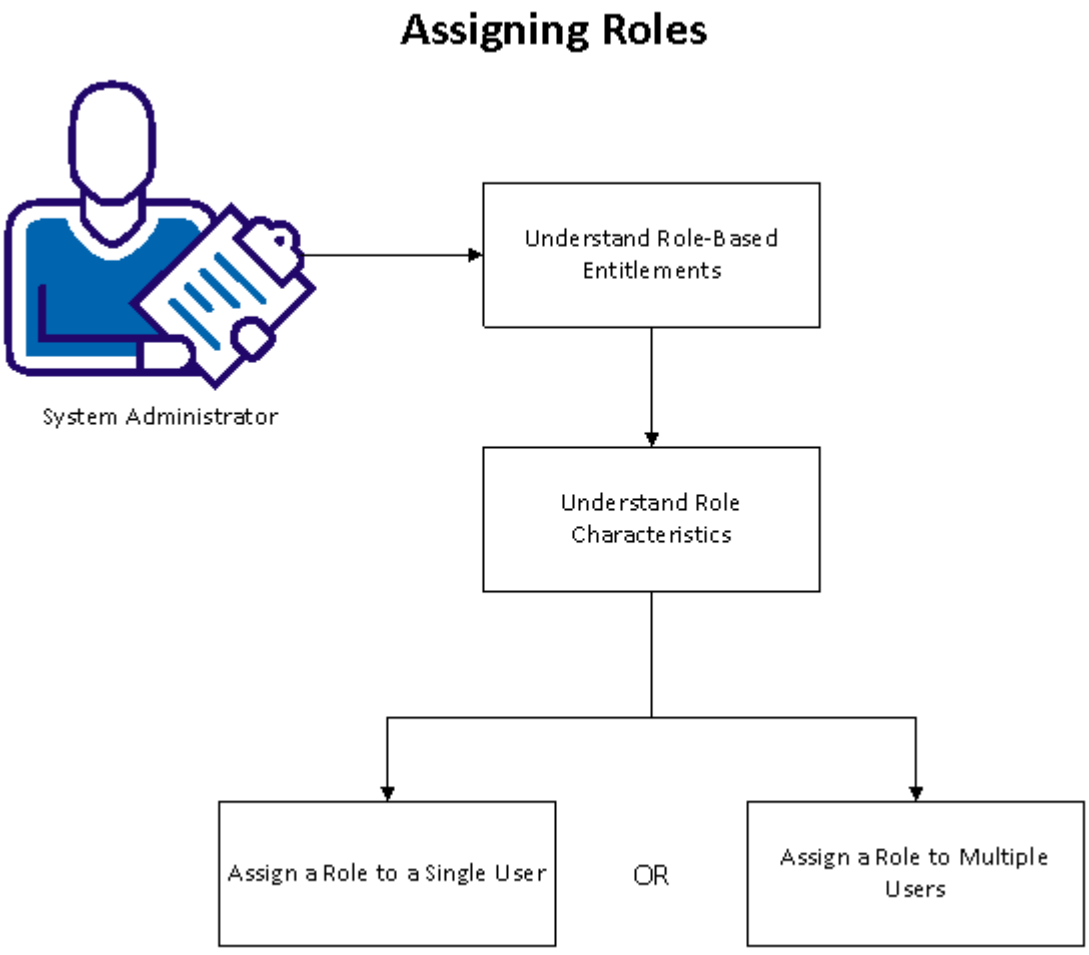
As a system administrator, you assign *admin roles* or *provisioning roles* to users. A user to whom you have assigned a role is called a role *member*.

You assign admin roles to grant and limit actions that users can take in CA CloudMinder. Users can perform administrative *tasks* on user accounts, such as changing a password or updating a job title. Different users have different levels of access to these tasks, which is based on their role membership. For example, with one role a user can only update their own personal information, whereas with another role, a user can administer account privileges for all users.

The admin role, or roles, that are assigned to a user determines which tasks the user can perform. A system administrator assigns a role to a user; that role defines a set of tasks that the user can then perform. The tasks in a given role are logically related to one another. For example, the Human Resources Manager role contains tasks to modify the name, address, title, and salary information. In addition, a user can have multiple roles, allowing you to organize efficiently the tasks each user can perform.

You assign provisioning roles to grant users access to accounts in additional applications, such as an email system. Provisioning roles contain account templates. These templates define the attributes that exist in a 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.

The following diagram shows the information to understand, and the steps to perform, in assigning roles.



The following topics explain roles in depth and how to assign them to users.

1. Understand Role-Based Entitlements (see page 111).
2. Understand Role Characteristics (see page 111).
3. Assign an Admin Role to a User (see page 94).
4. Assign a Provisioning Role to a User (see page 94).
5. Assign a Role to Multiple Users (see page 114).

Role-Based Entitlements

You assign privileges to users by assigning roles. A *role* contains tasks that correspond to application functions in Identity Management, such as the Create User task, functions in an application, such a Create Purchase Order function or account templates that give the user accounts, such as an SAP account. When users are assigned a role, they receive the corresponding privileges.

Identity Management provides the following types of roles:

- User management roles, which are called *admin roles*.

  Admin roles can also include any task that appears in the User Console.
- Account assignment roles, which are called *provisioning roles*
- Application function roles, which are called *access roles*.

If you remove a task or account template from a role, the user can no longer perform that task, use an endpoint account, or use an application function.

Role Characteristics

An admin role defines the tasks available to a user who has that role. A provisioning role defines the accounts that are assigned to members of that role. Both types of roles also contain rules that define who can have the role, who can administer or modify the role, and so on. When you assign a role to a user, the actions you are enabling the user to take, or the access to accounts you are granting, depend on how the role is defined.

The following table shows the characteristics that comprise a role. When you are preparing to assign a role to a user, understand the tasks, rules, and policies that are associated with that role.

Characteristics	Definition
Role Profile	Defines basic information about the role, such as the name and description.
Tasks	Defines the tasks that are associated with the role.

Characteristics	Definition
Account Templates	Define the details of accounts created in managed endpoints by a provisioning role.
Member Rules, Member Policies	■ A member rule defines conditions under which a user can be an admin role member. Admin role members can perform the tasks that are associated with a given role. ■ A member policy combines a member rule with scope rules.
Admin Rules, Admin Policies	■ An admin rule defines conditions under which a user can be a role administrator. Role administrators can assign a role to other users. ■ An admin policy combines an admin rule with scope rules and administrator privileges for assigning the role.
Owner Rules	Defines conditions under which a user can be a role owner. Role owners can modify a role. For example, they can add or delete tasks that are associated with that role.
Scope Rules	Limits the *objects* that members of a role can manage. Objects are users, groups, organizations, tasks and roles. For example, a role can allow role members to change salary information for other users. A scope rule can then limit those users to only ones within a specific department.
Add Actions, Remove Actions	Defines changes that are made to a user profile when a user is added or removed as a role member or administrator.

Assign an Admin Role to a User

You can assign admin roles to an individual user.

Follow these steps:

1. Log in to the User Console as a user with user management tasks.

   Note: The default User Manager role grants the appropriate tasks.

2. Select Users, Manage Users, Modify User.

   A search screen appears.

3. Search for a user to whom you want to assign the new role.

   To display a list of all users for whom you have administrative tasks, click Search without modifying the search criteria.

4. Select a user and click Select.

   The user profile appears.

5. Select the Admin Roles tab.
6. You can add an admin role from a list of available roles. You can also copy the role from a user that already has the desired role. Choose one of the following options:
   - Click Add an admin role, and search for the role you want to assign. A role only appears in the list of search results if you are an administrator of the role. Select the desired role and click Select.
   - Click Copy from a user, and search for a user that already has the desired role. Select the user, then select the desired role and click OK.

   An updated list of roles that are assigned to the user appears.
7. Click Submit.

   The user receives the specified roles.

Assign a Provisioning Role to a User

You can assign provisioning roles to an individual user.

Follow these steps:

1. Log in to the User Console as a user with the Modify Provisioning Role Members/Administrators task.
2. Select Roles and Tasks, Provisioning Roles, Modify Provisioning Role Members/Administrators.

   A search screen appears.
3. Select the role you intend to assign to the user.

   The Membership tab appears.
4. Click Add User.
5. Search for a user to whom you want to assign the role.

   To display a list of all users for whom you have administrative tasks, click Search without modifying the search criteria.
6. Select a user and click Select.
7. Select the Provisioning Roles tab.
8. Click Add a provisioning role, and search for the role you want to assign. A role only appears in the list of search results if you are an administrator of the role. Select the desired role and click Select.

   An updated list of roles that are assigned to the user appears.
9. Click Submit.

   The specified roles are assigned to the user.

Assign a Role to Multiple Users

You can assign roles to multiple users at once.

Follow these steps:

1. Log in to the User Console as a user with role administrator tasks.
2. Select Roles and Tasks.
3. Select either Admin Roles, Modify Admin Role Members or Provisioning Roles, Modify Provisioning Role Members/Administrators.

   The list of roles that you can manage appears. A role only appears in the list if you are an administrator of that role.
4. Select the role to which you want to add members, and click Select.

   A list of existing members or administrators appears.
5. Click the Add a User button.

   A search screen appears.
6. Search for the users to whom you want to assign the new role.

   To display a list of all users for whom you have administrative privileges, click Search without modifying the search criteria.
7. Select the desired users and click Select.

   An updated list of users who have this admin role appears.
8. Click Submit.

   The users receive the specified role.

Chapter 5: Access Request Services

This section contains the following topics:

Create a Service Using the Service Wizard

Services simplify *entitlement* management. A service bundles together all the entitlements - applications, roles, groups, and attributes - a user needs for a given business role.

For example, all new sales employees need secure access to Salesforce.com and a Salesforce.com account. They need membership in the CA CloudMinder Sales group. They also need specific information added to their user account profiles. An administrator creates a service named Sales Administration that combines the required application, roles, group, and profile attribute information. When an administrator assigns the Sales Administration service to a user, the user becomes a *member* of the service. The user receives the entire set of entitlements that you define in the service.

As an administrator, a key use of services is to give users access to the software resource defined by an application. To give users this access, create a service that includes the application, then make the service available to users.

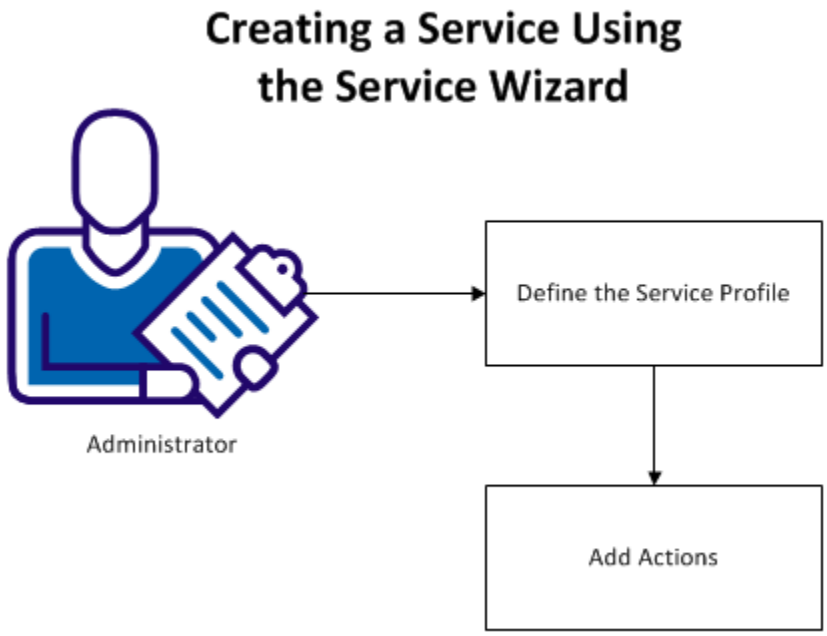
Users access the software resource in the manner that is defined in the application. For example, you can configure the application for Single Sign-on, or you can protect it with your choice of authentication method. Users who access the application through a service receive the benefit of these configurations.

You make the service available various ways. You can assign a service directly to one or more users. You can configure the service so that an application icon appears in the User Console of service members. Users can click the icon to access the application. Users can also request access to a service themselves through the User Console. For more information, see Make a Software Resource Available to Users.

Note: As an administrator, you can also give users access to an application by making a link to the application available. For example, you can insert the link into any web page or you can send the link in an email. For more information, see Creating a Service: Service Wizard.

The simplest way to create a service is by using the service wizard.

The following diagram shows the steps to perform, to create a service through the service wizard and make it available to users.



The following topics explain how to create a service using the service wizard:

1. Define the Service Profile (see page 117)
2. Add Actions (see page 118)

Define the Service Profile

On the Profile tab, you define basic characteristics of the service.

Follow these steps:

1. Log in to an account that has service management privileges.

   For example, the default Tenant Administrator role has the appropriate privileges.

2. From the navigation menu, select Services.
3. Click Service Wizard, Create Service.

   The Create Services screen appears.

4. On the Profile tab, enter a name and tag. A tag is a unique identifier for the service.

   Note: Tags can only contain alphanumeric and underscore characters, and cannot start with a number. Once created, a tagname cannot be changed, or reused, even if a service is later deleted.

5. Select Enabled if you want to make the service available to users as soon as you create it.
6. If you want this service to appear in the list of services available for users to request, select Self Subscribing. When Self-Subscribing is enabled, users can request access to this service through the User Console.
7. (Optional) Add one or more categories. Type a category name and click the up arrow to add it to the service.

   Categories add more information to a service. You can use this additional information to facilitate service searches in environments that include a significant number of services.

Add Actions (Service Wizard)

On the Actions tab, you define what entitlements are granted to the user - for example, access to an application, or membership in a role or group - when a user receives the service.

On the Actions tab, from the drop-down menu, select one or more of the following actions:

Application

Service members receive access to the selected application. The system applies group membership or rule string configuration for the application, if necessary. For more information, see Creating an Application (see page 123).

Launch Role

The system adds a link and icon for the application in the User Console of service members. This action need only be added when you want to give users access to an application through this service. Select one of the following options:

Create a new launch role for an application

Select the application that you want service members to be able to access, and enter a name for it. The system adds an icon with this name in the User Console Home page of service members. The system also adds a link with this name in the left-hand navigation pane of the User Console of service members. The icon and the link both launch the application.

Create a new launch role

This action is the same as creating an admin role. If you have task administration privileges, you can add one or more tasks to this role through the Modify Admin Role task. The system then adds a link to these tasks in the left-hand navigation pane of the User Console of service members. For more information, see Admin Roles and Tasks.

Select an existing launch role

Select the launch role that you want service members to be able to access. This role can be a launch role for an application, or for any admin role.

Provisioning Role

Service members receive the selected provisioning role. The system creates an account for the user in the endpoint that is configured in the provisioning role when a user receives the service. For more information, see Creating Roles to Assign Accounts.

Group

The system adds service members to the selected group.

Attribute

The system adds the indicated attribute to the user accounts of service members.

The system adds each action that you select to the service. When a user receives access to the service, the system applies each action to the user. For example, the user receives the indicated Launch Role, and access to an application in their User Console Home page.

Important! You can set the order of actions in a service. If you add actions that affect user attributes, and have a provisioning action in the service, order is important. Place actions that affect attributes **before** any provisioning actions in the action order. The Attribute action can affect user attributes. The Application action can also affect user attributes, if a rule string is configured for the application.

Note: Typically, the application and provisioning role you select while creating a service are closely related. The application makes a specific software resource available in the system. The provisioning role creates a user account in the same software resource. Thus, when a user receives the service, they automatically receive access to the software resource through their User Console, and an account in the same software resource.

When you have added all desired actions to the service, click Submit. The system creates a service with the selection actions. When a user receives access to the service, the user receives access to the selected application. The user also receives all roles, groups, and attributes you included in the service.

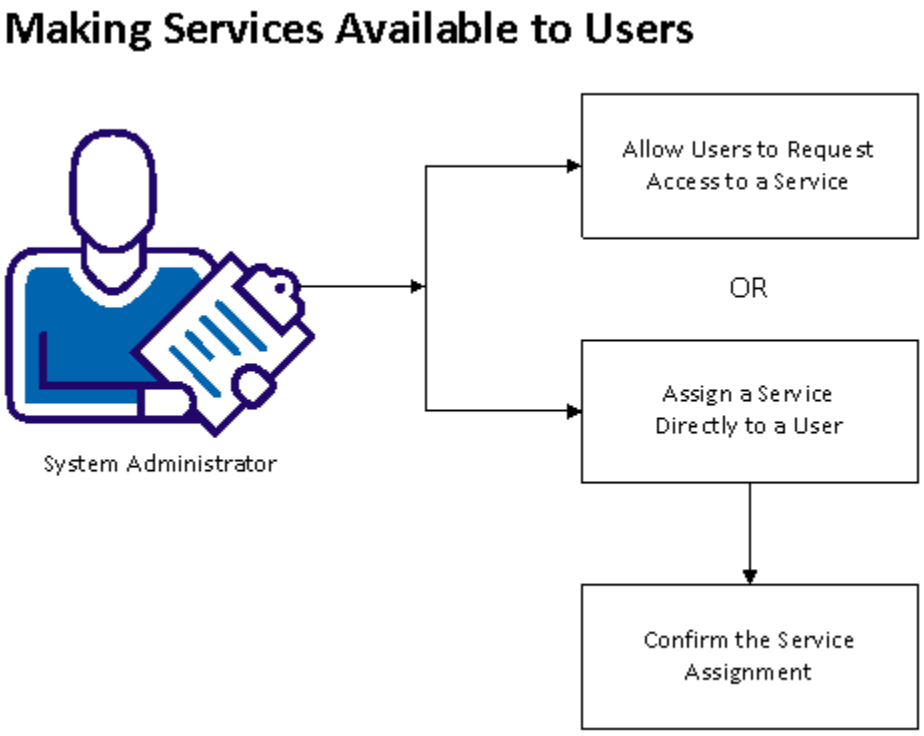
Making Services Available to Users

Services simplify entitlement management. A Service bundles together all the entitlements a user needs for a given business role. Services are available to the user through Access Request tasks in the User Console. Access Request tasks enable a user or administrator to request, assign, revoke and renew a Service through the user interface.

Services allow a system administrator to combine user activities and information - tasks, roles, groups, and attributes - into a single package, which are managed as a set. For example, all new Sales employees need access to a defined set of tasks, accounts on specific endpoint systems, and specific information added to their user account profiles. A system administrator creates a service named Sales Administration, containing all the required tasks, roles, groups, and profile attribute information for a new Sales employee. When an administrator assigns the Sales Administration service to a user, that user receives the entire set of roles, tasks, groups and account attributes that are defined by the service.

Another way users can access services is to request access themselves. In the User Console, each user has a list of services available for their request. This list is populated with services marked as "Self Subscribing" by a system administrator with the appropriate privileges, typically during service creation. From the list of available services, users can request access to the services they need. When the user requests access to a service, the request is fulfilled automatically. The associated tasks, roles, groups and attributes are assigned to the user immediately. A CA CloudMinder administrator with the appropriate privileges can also configure service fulfillment to require workflow approval, or to generate email notifications.

The following diagram shows the information to understand, and the steps to perform, to make services available to users.



You can make services available to users using the following methods:

1. Allow users to request access themselves.

   In the CA CloudMinder User Console, when the user clicks My Access, then Request & View Access, the user sees a list of services available for their request. The services that appear in this list are those marked "Self Subscribing" by a CA CloudMinder administrator with the appropriate privileges, typically during service creation.

   When the user requests access, the system assigns the service to the user. The user receives all applications, roles, groups and attributes associated with the service. If the service includes a Launch Role for an application, an icon and a link to the application appear in the User Console Home page.

2. Assign a Service Directly to a User (see page 95).

3. If you assign a service directly to a user, Confirm the Service Assignment (see page 122).

Assign a Service to a User

You can assign a service directly to an individual user. This user becomes a *member* of the service.

Follow these steps:

1. Navigate to Services, Request & View Access.

   A list of services you can administer appears.

2. Select the service that you want to assign to a user and click Select.

   A list of users that are assigned to the service appears.

3. Click Request Access.

4. Search for a user to whom you want to assign the service.

   To display a list of all users for whom you have administrative privileges, click Search without modifying the search criteria.

5. Select a user and click Select.

   An updated list of users that are assigned to the service appears.

6. Click Save Changes.

   The user receives the specified service. The user receives all applications, roles, groups, and attributes you included in the service.

Confirm Service Assignment

Once you have assigned a service to a user, confirm that all tasks associated with the service completed successfully.

Follow these steps:

1. Navigate to Services, View Service Access Request History.

   A search screen appears.

2. Search for the service you assigned to a user.

   To display a list of all services over which you have administrative privileges, click Search without modifying the search criteria.

   A list of services you can administer appears.

3. Select the service that you assigned, and click Select.

   A history of actions that is associated with the service appears.

4. Click Last Changed to see the most recent actions first.
5. Confirm that the user in question received the service successfully.
6. Click Close.

Renewing Access to a Service

Some services expire after a certain period of time. Administrators can renew a service for users to prevent an interruption in their access.

You can renew a service using one of the following methods:

- Select the service, then select the user access to renew
- Select the user, then select the service to renew

Note: Depending on how an environment is configured, end users can also renew their access by using the Renew Access task.

The following procedure describes how to renew access by selecting the service first. If you want to select the user first, use the User Access Requests, Manage User Renew Requests task in the Users category.

Follow these steps:

1. Click Services, Renew Access in the User Console.
2. Search for and select the service that you want to renew.

   The User Console displays a list of users who currently have access to the service you selected, and the date their access expires.

3. Select the duration for the renewal in the Access Request column, then click OK.

   The options in the Duration field are determined when the service is created.

4. Click Save Changes.

You can view the status of the service renewal by using the View Access Request History in the User Console.

Enable Workflow for Access Request Tasks

The following default tasks allow users to request or revoke access to services:

- Request And View Access
- Manage User Access Requests

To enable workflow for access request tasks, you configure global policy-based workflow.

Follow these steps:

1. Select System, Configure Global Policy Based Workflow.
2. Add one or more of the following events, and configure workflow for them:
   - AddServiceToUserEvent
   - RemoveServiceFromUserEvent
3. Click Submit.

Create an Application

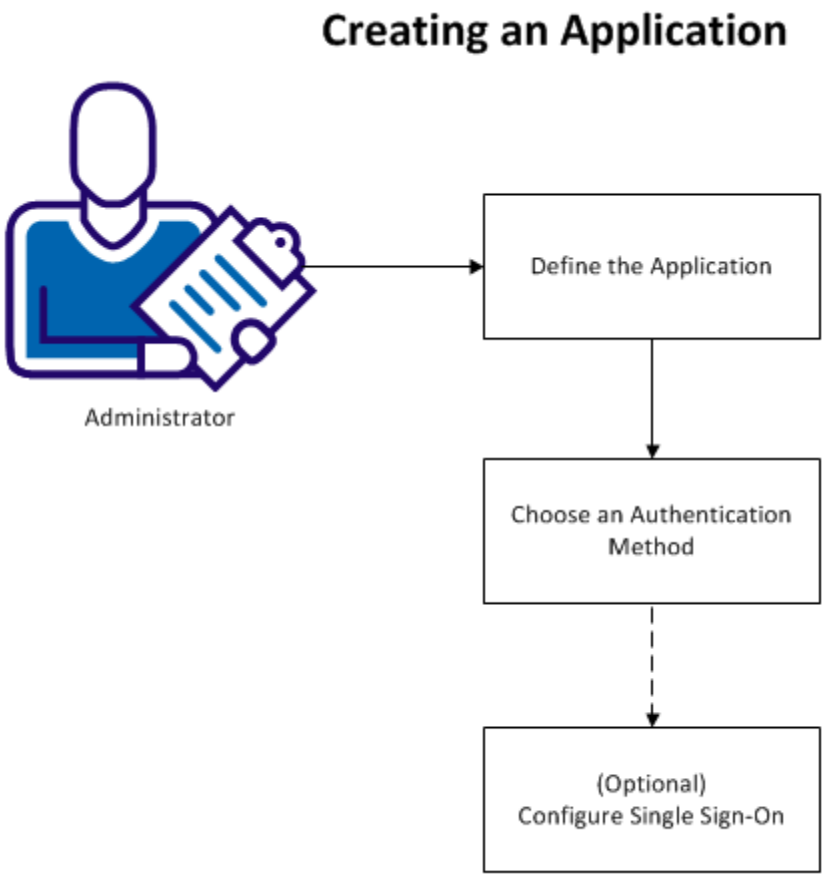
As an administrator, you want to give your users secure and convenient access to software resources. For example, your users need access to your email system, which can be hosted on-premise by your organization. Users also need access to Salesforce.com, which an external organization hosts in the cloud.

Note: Although a tenant administrator typically creates applications for their environment, a hosting administrator can also perform this task.

You create an application to define how users access a software resource. For example, when you configure an application, you define what type and level of security protects the resource. If you have purchased CA CloudMinder Advanced Authentication, you can configure advanced security such as two-factor authentication to protect the resource. If you have purchased the CA CloudMinder Single Sign-on service, you can configure SSO for the application. Users only log in once to access all applications that are configured for SSO.

Once an application is configured, you can give users access to the software resource. You can configure a service that includes the application, and can assign the service to users. The users can click the icon in the User Console Home Page to access the application. For more information, see Creating a Service Using the Service Wizard (see page 115). You can also give users access to the application by making a link to the application available. For example, you can insert the link into any web page or you can send the link in an email.

The following diagram shows the information to understand and the steps to perform to create an application and make it available to users.



The following topics explain how to create an application:

1. Define the Application Profile (see page 60)
2. Choose an Authentication Method (see page 126)
3. (Optional) Configure Single Sign-On (see page 128)

Define the Application

You define the application details through the User Console.

Follow these steps:

1. Log in with an account that has application management privileges.

   For example, the default Tenant Administrator role has the appropriate privileges.

2. From the navigation menu, select Applications.
3. Click Applications, then Create Application.

   The Create Application screen appears.

4. Enter a name and description.
5. Associate a group with the application, if desired.

   If you specify a group on an application, use the Service wizard to create a service for the application, where there is a rule written to add\remove the requested user(s) to that group. When the service is assigned, the requested user will be a member of the group. When the service is revoked, the user will be removed from the group.

   Note: If you are configuring the application for SSO access, the group that you choose must match the group name that is indicated in the SSO partnership configuration for this application. To confirm the group name that is indicated in the partnership configuration, refer to your hosting administrator. SSO partnership configuration information is available in the CSP Console.

6. Enter a launch URL for the Application.

   A launch URL is the fully qualified domain name of the software resource you want to make available to users. For example, if a user clicks the icon for this application in the User Console Home page, they are directed to the launch URL.

   If you are configuring the application for SSO access, the launch URL is the SSO Service URL generated during SSO partnership configuration. Refer to your hosting administrator for this information.

   If you are not configuring an SSO application, simply enter the fully qualified domain name of the software resource. Use the following format:

   https://softwareresourcedomainname.com

7. Choose a logo.

   This logo is the icon for the application that appears in the User Console Home page. Users can click the icon to access the software resource.

   Note: You can also give users access to the application by inserting a link to the application into any web page.

8. Enter a welcome message.

   When users click any link you provide to the application, a login screen appears. The welcome message appears at the top of this screen.

9. Select a self-registration task.

   If a user attempts to access the application but the user does not have a CA CloudMinder account, you can allow them to self-register. Choose one of the following self-registration tasks:

   Create New Account

   Presents a simple registration form. Upon submission, creates a user account.

   Create New Account with Workflow

   Presents a simple registration form. Upon submission, forwards the user account request to one or more approvers. Creates an account upon approval.

   Create New Account with Domain Validation

   Presents a simple registration form. Upon submission, compares the email domain of the user to the tenant email domain. If they match, sends a confirmation email to the user. Creates an account upon user confirmation.

   Note: The tenant email domain is specified in the User Console, under Tenant Administration, Tenant Settings.

   Self-Registration with Attribute Exchange

   Do not choose this self-registration task in the context of application access. This task is intended for a separate purpose.

10. Choose an authentication method. (see page 126)

Choose an Authentication Method

In the Create Application screen, continue the process of creating an application by choosing one or more authentication methods. When a user attempts to access the application, the system presents a login screen. The authentication methods that you choose appear on this screen. The user can log in using their choice of the available authentication methods.

For example, you can select the Basic and Google External IDP authentication methods for an application. The application login screen displays user name and password fields for basic authentication. The login screen also displays the Google icon, so users can log in with their Google credentials.

Follow these steps:

1. In the Authentication Methods area, click Add.

   The Select Authentication Methods screen displays a list of the authentication methods available in the tenant environment.

   Note: First, create authentication methods in the system before you perform this step. You define authentication methods through the User Console, using the Authentication Methods tasks. For more information, see Create Authentication Methods.

2. Select one or more authentication methods. The following types of authentication method are available:

   Basic

   Offers simple user name and password login.

   External IDP

   Offers log in through an external credential provider, such as Google or Facebook.

   Advanced Authentication

   Offers advanced authentication methods that have been configured for your environment, such as One Time Password (OTP) authentication.

   Note: Advanced Authentication methods only appear if you have purchased the Advanced Authentication Service.

   You can choose as many authentication methods, of any type, as you want. All the methods that you select are displayed on the login page that appears when a user attempts to access the application.

3. Click Select.

   The Create Application screen appears, updated with the list of authentication methods you selected.

4. (Optional) From the drop-down list, choose a default authentication method.

   Note: Advanced Authentication methods are never available as a default.

5. Configure Single Sign-On (see page 128).

(Optional) Configure Single Sign-On

Note: The option to configure single sign-on settings only appears in the User Console if you have purchased the SSO service.

During partnership configuration for an SSO application, a hosting administrator specifies a *federation attribute* for the partnership. The system uses this attribute to exchange information with the target software resource during single sign-on operations. For example, when configuring an SSO partnership between CA CloudMinder and salesforce.com, a hosting administrator chooses User ID as the federation attribute. The system retrieves this attribute from the database and forwards it in a SAML assertion to salesforce.com to facilitate single sign-on.

Some target software resources require the federation attribute to have a specific format. If this format differs from the format CA CloudMinder uses for the attribute, use the following steps to set the attribute value to the required format. This process is named setting the rule string for the attribute.

Note: Only configure the rule string if the software resource requires that the attribute take a format different from the way it is stored in the CA CloudMinder database.

Follow these steps:

1. In the Create Application screen, click Configure Single Sign On settings for the application.

   The Single Sign On configuration settings appear.

2. Select the Federation User Attribute.

   The attribute that you choose must match the assertion attribute that is indicated in the SSO partnership configuration for this application. If the attribute names do not match, users cannot successfully access this application through SSO. To confirm the assertion attribute name that is indicated in the partnership configuration, refer to your hosting administrator. SSO partnership configuration information is available in the CSP Console.

3. Configure the rule string for the Federation User Attribute.

   The rule string is the format that you want the attribute to take when the system passes it to the target software resource.

   Note: To learn the exact format that is required for this attribute, refer to your hosting administrator, or an administrator at the target software resource.

You have created an application and applied an authentication method. You have also configured single sign-on settings if applicable. You can now include this application in a service so that users can access the application.

Deleting an Application

You can delete an application you no longer require.

Follow these steps:

1. Log in to the User Console.
2. Select Applications, Application, Delete Application.
3. Search for the application you want to delete.
4. Select the application and click Select.

   A confirmation message appears.
5. Click Yes.

   The application is deleted.

Chapter 6: Bulk Operations

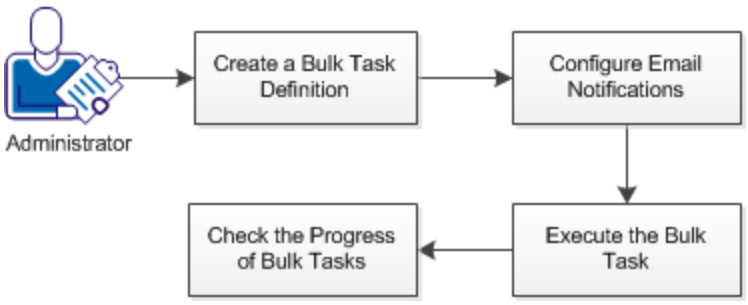
This section contains the following topics:

How to Modify Multiple Objects (Bulk Modify)

You can use bulk tasks to perform the following actions:

- Run a task on an object, such as User, based on the attributes of the object, such as department, city, termination date, and so on.
- Run a task on specific objects periodically, such as every Saturday.
- Make bulk user changes, such as modifying all users within a selected department.

This functionality differs from the scheduled task functionality by providing a population filter. Unlike scheduled tasks, the population of objects affected by the bulk task is unknown when you configure the bulk task. Also, bulk tasks affect many objects, while scheduled tasks only affects one.



Follow these steps:

1. Create a Bulk Task Definition (see page 132).
2. (Optional) Configure Email Notifications for Bulk Tasks (see page 135).
3. Execute the Bulk Task (see page 136).
4. Check the progress of Bulk Tasks (see page 137).

Create a Bulk Task Definition

To run a bulk task, first create a bulk task definition. In the User Console, navigate to System, Bulk Tasks, Create Bulk Task Definition. The following components make up a bulk task definition:

- The initiator of the task
- The object type
- The task to perform
- The population filter

Bulk Task Profile Tab

The Profile tab allows you to define the initiator of the bulk task, the task performed, and the object type to perform the task on. The following fields must be configured:

Name

Defines the name of the bulk task.

Description

Explains the use case for the bulk task.

Initiator

Defines the user who runs the bulk task once it is triggered. By default, the Initiator is set to the user defining the bulk task.

The default user scope of the Bulk Task Manager role only allows a user to set themselves as the initiator. This limitation prevents security issues, such as users disguising their identity by setting the initiator to another user when running bulk tasks.

However, you can use this field to run a bulk task as another user, for example, a system administrator running a bulk user task on behalf of the Human Resources director. To allow bulk task users to change the initiator to another user, change the user scoping of the Bulk Task Manager role.

Note: The user you choose as the initiator affects the tasks available and the population filter results, as both are based on the initiator's scope.

Object Type

Defines the type of object that the bulk task modifies. You can add object types to the drop-down list, by modifying the Object Types field in the Profile tab configuration. To modify the Profile tab configuration, modify the admin task that includes the drop-down list, select the Tabs tab, and edit the Profile tab.

Default: User object types only.

Note the following:

- If you add object types, be sure to modify the Profile tab of both the Create *and* Modify tasks.
- If you add object types, be sure to add scope rules for that object type on the role.

Task

Specifies the task to perform on the objects that match the population filter. This task list includes most admin tasks, except the following:

- Tasks of type View or Create (such as View User and Create User)
- Approval tasks

Note: Not all tasks are available for all users. The list of tasks depends on the object type and the initiator's scope.

(Optional) Attributes

Define a list of attributes (see page 133) to set on objects that match the population filter. These attributes are useful with tasks that involve attribute changes, such as Modify User. For example, you can select Department Name as the attribute and 'Sales' as the value, and for every user that matches the population filter, the system changes the Department Name attribute to Sales.

Set Optional Attributes

You can add optional attributes if you want to make attribute changes on any object found in the population filter.

To set optional attributes

1. Click the Attributes button.

   A drop-down list of the attributes associated with the task appears.

2. Select the attribute you want to set.

3. Click Add (plus button).

   A new line appears in a table with an empty Values text box next to the attribute.

4. Enter the values you want to set on the attribute.

5. Repeat Steps 2 through 4 for any attribute you want to set.
6. Click Ok.

Note: When you select a multi-valued attribute, you can click the Add (plus) button to set multiple values for that attribute.

Bulk Task Population Tab

The Population tab allows you to find objects for which the bulk task applies. You can define the population filter with the following fields:

Object Filter

Defines the object population using standard filters. The attributes available for the search are based on the object type selected on the profile tab of the bulk task.

Date Filter

Refines the population filter further using attributes that contain dates (see page 134), such as a hire date attribute.

Date Format

Defines the date format that the date filter uses.

Preview

Displays a list of objects that meet the population filter criteria when the Preview button is clicked. This Preview button helps verify that the filter is configured correctly, but the population can change over time. Therefore this list should *not* be used to indicate objects that will be changed in the future.

Note: System filters put a higher priority on the OR operator than the AND operator. For example, "City equals NYC **AND** Department equals Sales **OR** Department equals Purchase" is treated as "(City equals NYC) **AND** (Department equals Sales **OR** Department equals Purchase)".

Date Filter Components

Filtering on dates within bulk tasks is useful as the population can change daily. For example, an object filter that searches for users whose expiration date has passed can change every day.

Important! If objects are in an LDAP user store, date searches may cause a significant performance reduction due to the dates being represented as regular strings.

The following fields make up the date filter:

Attribute

Defines an attribute in the object that contains a date. All attributes for the object are available. If the filter uses an attribute, the system assumes the attribute contains a date.

Attribute values must match the date format set in the population tab. Objects that have an invalid date format will be ignored.

Operator

Refers to past or future dates compared to today.

Day Offset

Defines a lag time from today. For example, if you want to send an email to all users whose profile expires in the next week, the operator is 'Today or earlier' and the offset is 7, indicating 7 days from today. If you set the offset to -7, however, the email is sent to all users expired for more than a week. The following table outlines the behavior of the offset:

Today's Date	Operator	Day Offset	Result
1/10/2010	Today or Earlier	7	Any date on or before 1/17/2010
1/10/2010	Today or Earlier	-7	Any date on or before 1/3/2010
1/10/2010	Today or Later	7	Any date on or after 1/17/2010
1/10/2010	Today or Later	-7	Any date on or after 1/3/2010

Configure Email Notifications for Bulk Tasks

In some environments, bulk operation email notifications are configured by default. To check if bulk operation email notifications are configured in your system, go to System, Email, View Email, and search on the term 'bulk'.

If no email notifications are configured in your environment, configure the email that is sent when a bulk operation completes.

Follow these steps:

1. Navigate to System, Email, Create Email in the User Console.
2. Complete the required fields on the Profile tab.

3. On the When to Send tab, complete the following steps:
   a. Select Task Completes in the first field.
   b. Select Execute Bulk Task in the second field.
4. Complete the Recipients and Content tabs, then click Submit.

   Email notifications are configured for bulk tasks.

Execute a Bulk Task

The Execute Bulk Task task allows you to schedule a bulk task or manually start a bulk task right away. Bulk tasks are usually scheduled, but starting a bulk task manually does not interfere with any scheduling already configured on the bulk task, and the bulk task runs immediately. Once you select Execute Bulk Task, select Execute now to start the bulk task manually.

To schedule a bulk task (see page 136) to run periodically, use the recurrence functionality. Once you select Execute Bulk Task, select Schedule new job and choose the options that you want.

The Preview button allows you to see what objects will be affected by the bulk task before starting it.

Note: If your bulk task population includes 500 objects, 500 nested tasks are created; one for each object. For performance reasons, we recommend scheduling bulk tasks with large populations.

Recurrence Tab

Use this tab to schedule your job. The fields in this tab are as follows:

Execute now

Runs the job immediately.

Schedule new job

Schedules a new job.

Modify existing job

Specifies that you want to modify a job that already exists.

Note: This field appears only if a job has already been scheduled for this task.

Job Name

Specifies the name of the job you want to create or modify.

Time Zone

Specifies the server time zone.

Note: If your time zone is different from the server's time zone, a drop-down box is displayed so you can select either your time zone or the server's time zone when scheduling a new job. You cannot change the time zone when modifying an existing job.

Daily schedule

Specifies that the job runs every certain number of days.

Every (number of days)

Defines how many days between job runs.

Weekly schedule

Specifies that the job runs on a specific day or days and time during a week.

Day of Week

Specifies the day or days of the week the job runs.

Monthly schedule

Specifies a day of week or day of month that the job runs on a monthly basis.

Yearly schedule

Specifies a day of week or day of month that the job runs on a yearly basis.

Advanced schedule

Specifies additional scheduling information.

Cron Expression

For information about filling out this field, see the following:

http://quartz-scheduler.org/api/2.1.0/org/quartz/CronExpression.html

Execution Time

Specifies the time of day, in 24-hour format, that the job is run. For example, 14:15.

Check the Progress of Bulk Tasks

You can check the progress of bulk tasks by using the following methods:

- Viewing status in View Submitted Tasks

  The View Submitted Tasks screen shows a summary of bulk operations. The summary includes the total number of tasks, the number of completed tasks, and the number of remaining tasks. The summary also provides information about the number of tasks in Completed, In progress, and Audited states.

- Receiving email notifications that are sent when a bulk operation completes.

Bulk Task Recovery

If a failure occurs while the event is running, the main bulk task event shows as Failed. You can resubmit the bulk task event (through View Submitted Tasks) which causes the system to restart the bulk task at the place where the failure occurred.

Use Case: Bulk User Changes

You want to perform a mass change so that all users in the Sales department will now be in the Purchasing department.

1. Under the Profile tab of Bulk Tasks, create a bulk task definition with the name Change To Purchasing.
2. Set the object type to user.
3. Select Modify User as the task to run.
4. Click Attributes and set the value of department to 'Purchasing.'
5. Under the Population tab, set 'department equals Sales'.
6. Select Execute Bulk Task to run the definition immediately.

Use Case: Using Attributes that Contain Dates

You want to create an automated process to disable temporary users twenty days before their termination date.

1. Under Tasks, System, Bulk Tasks, create a bulk task definition with the name Disable Contractor.
2. Set the object type to User.
3. Set the task to perform as Disable User.
4. Enter the following values in the date filter:
   - Attribute: Termination Date
   - Operator: Before Today
   - Disposition: 20

   You can add any other attribute in the population filter, such as Employee Type = Contractor. In this case, only contractors are affected.

Manage Tenant Bulk Operations

As an administrator, you can manage tenant bulk operations to prevent one tenant from consuming all available system resources.

When managing tenant bulk operations, you can configure the following options:

- **Default:** Workflow

  When a tenant submits a bulk operation, it is sent for approval by the hosting administrator.

  Note: For more information on workflow, see the *Identity Management Administration Guide*.

- Quotas

  When a tenant submits a bulk operation, it is limited by a quota that is set by the hosting administrator. Once the bulk operation quota is reached, the remaining bulk tasks are queued until the quota is renewed.

  Note: For more information, see How to Configure Tenant Bulk Operation Quotas (see page 139).

- Both Workflow and Quotas

  When a tenant submits a bulk operation, it is first sent for approval by the hosting administrator. Once approved, the bulk operation is limited by the quota limits set.

How to Configure Tenant Bulk Operation Quotas

As an administrator, you can define a quota to limit the number of bulk operations that a tenant administrator can submit during a specific time period. Functionality that is affected by these limits includes bulk tasks, bulk loader, and the bulk load client. Establishing a bulk operation quota prevents one tenant from consuming all available system resources.

If a tenant administrator reaches a quota for a given time period and tries to submit another bulk operation, the task is put into a scheduled state until the quota is reset. Also, an email is sent to the administrator and the tenant to inform them that the tenant has reached the quota.

Note: Log in to the tenant environment to modify the task quota for a specific tenant.

Follow these steps:

1. In the User Console, go to System, Manage Task Quota.
2. Click Create Task Quota and create an object of type Task Quota.

3. Enter the following information

Task Name

Defines the bulk operation that you want the quota to apply to.

Quota

Specifies the maximum number of bulk operations you can submit in a certain time period.

Duration

Defines the numerical value of the time until the quota is reset.

Note: We recommend a minimum duration of 30 minutes. A shorter duration may cause task submission issues.

Interval

Defines the time interval for the duration value.

Start Time

Defines the time when the quota becomes available to the tenant administrator. Any bulk operation submitted before this time is queued.

Time Zone

Specifies the time zone for the Start Time. This field should be set to the tenant administrator time zone.

4. Click Submit.

How to View Used Task Quota

As an administrator, you may have access to bulk operation tasks. These operations are limited so that you can only submit a specified number of bulk operations during a specific time period. Functionality that is affected by these limits includes bulk tasks, bulk loader, and the bulk load client.

If you reach a quota for a given time period and try to submit another bulk operation, the task is put into a scheduled state until the quota is reset.

Follow these steps:

1. In the User Console, navigate to System, Manage Task Quota.
2. Click View Used Task Quota and search for the task quota you want to display.

   The Task Quota table appears and displays your used quota.

Note: You can use View Submitted Tasks (VST) to view how many bulk operations are completed compared to how many bulk operations are scheduled.

Aborting Bulk Operations

If you want to abort a bulk operation while viewing the task status in View Submitted Tasks (VST), click Abort. Aborting the bulk operation stops all task submission. Any tasks that are already submitted by the bulk operation are allowed to complete.

Chapter 7: Reporting

This section contains the following topics:

How to Enable Reporting for Tenant Administrators

Reporting tasks are available as tasks in the User Console. For example, the Advanced Authentication service provides a number of reports that capture details of transactions performed by end users authenticating with the service and also record day-to-day operations performed by the administrator. Other tasks provide reports on the Identity Management and SSO services.

Reporting tasks for Identity Management service are available to the tenant administrator with no additional configuration. However, for the Advanced Authentication and SSO service, you perform additional configuration to provide that administrator with reporting tasks.

This section describes how the hosting administrator associates Advanced Authentication and SSO reports tasks with the tenant administrator role.

Prerequisites to Enabling Reporting

Before you begin performing the tasks that are described in this scenario, ensure that the following prerequisites are addressed:

- The administrator must possess knowledge of the concepts and management tasks that are related to reports.

  Note: For information about the reporting feature, see the Identity Management documentation.

- This section is addressed to the hosting administrator. However, the procedures described in this section can be performed by any administrator to whom the privileges to create roles and tasks have been assigned.

Enable Advanced Authentication Reporting

This section describes the pre-configuration steps for required for enabling Advanced Authentication reports tasks.

Configure the Database for Advanced Authentication Reporting

1. Install the Oracle client on the Report Server.
2. Add the advanced authentication database details to the tnsnames.ora file.
3. Change directory to *JBoss*/server/all/deploy/iam_im.ear/user-console.war/reports.
4. Copy cam-aa-oracle-postgresql-reports.biar to the *im_admin_tools_dir*/ReportServerTools folder.
5. Copy the sample XML from /opt/reports to im_admin_tools_dir/ReportServerTools folder
   - For **Oracle**: AA Oracle sample.xml
   - For **PostgreSQL:** AA postgres sample.xml
6. Edit the values in XML file, which are marked in italics in the following example:

```
username>please specify the Arcot DB User</username>
            <password>please specify the Arcot DB User
Password</password>
            <datasource>please specify the Alias
name</datasource>
            <server>please specify the DB server:1521</server>
            <jdbcurl>jdbc:oracle:thin:@please specify the DB
server:1521:please specify the Alias name</jdbcurl>
```

7. Run the BIconfig utility on AA Oracle sample.xml or AA postgres sample.xml to export cam-aa-oracle-postgresql-reports.biar into the Report Server. Use this command format:

```
./biconfig.sh -h "hostname" -u "administrator_name" -p
"administrator_password" -f "<AA Oracle/Postgres Sample>.xml"
```

Enable the Advanced Authentication Roles

1. Log in to the User Console as the CSP administrator.
2. Select Roles and Tasks, Admin Roles, Enable/Disable Admin Role.
3. Select the check box to enable the Advanced Authentication Manager role.
4. Select the check box to enable the Advanced Authentication Reports User role.
5. Click Select.
6. Click Yes to confirm.

   The system enables the Advanced Authentication Manager and the Advanced Authentication Reports User roles.

Give Tenant Administrators the ability to use Advanced Authentication Reports

1. Log in to the User Console as the CSP administrator.
2. Select Roles and Tasks, Admin Roles, Modify Admin Role.
3. Select Advanced Authentication Reports User role and click Select button.
4. On the Members tab, under member policies, click Add.
   a. Select this option: who are members of <role-rule> as the Member Rule
   b. Select Admin Role.
   c. Click Browse to select Tenant Administrator role.
   d. Click Okay.
5. Click Submit.

Complete the configuration

For advanced authentication, the SQL files are available on Identity Management server.

1. Change directory to this location:
   `/opt/jboss-eap-5.1.2/jboss-as/server/all/deploy/iam_im.ear/user_console.war/reports`
2. Extract the ZIP file that applies to your database:
   `PostgreSQL – cam-aa-postgresql-db-scripts.zip`
   `Oracle - cam-aa-oracle-db-scripts.zip`
3. For Oracle, run the scripts as the Arcot database user in the following sequence:
   `ca_reportstrings-oracle-create.sql`
   `ca_reportstrings-oracle-insert_stmts_english.sql`
   `ca_ui_customization-oracle-create.sql`
   `ca_ui_customization-oracle-insert_stmts.sql`
   `im-oracle-audit_start_date.sql`
   `im-oracle-audit_end_date.sql`
4. For PostgreSQL, run the scripts as the Arcot database user in the following sequence:
   `ca_reportstrings-postgresql-create.sql`
   `ca_reportstrings-postgresql-insert_stmts_english.sql`
   `ca_ui_customization-postgresql-create.sql`
   `ca_ui_customization-postgresql-insert_stmts.sql`
5. For PostgreSQL, run the following scripts as Identity Management Object Store Database User:
   `im-postgresql-audit_start_date.sql`
   `im-postgresql-audit_end_date.sql`

Now the tenant administrator can request advanced authentication reports in the User Console.

Enable SSO Reporting

This section describes the pre-configuration steps required for enabling SSO reports tasks.

Set Logging to a Database or text file

The same setting which exists in smconsole for the access log is needed for CA CloudMinder access data. In the smconsole data tab, select either the database or a text file.

If the audit logging is to a text file, the CA CloudMinder access data is redirected to smaccess.log.

Enable Logging

1. Access the smconsole.
2. Select the data tab.
3. Locate the database drop down.
4. Select Audit Logs.
5. Locate the storage drop down and select ODBC.
6. Enter the data source information. Alternatively, select the Policy Store Database check box.
7. Check the logs tabs.
8. In the Policy Server Audit Log section, enable events to be logged.

   Select items to log and choose Log All Events.
9. Restart SiteMinder.

Push Data offline from smaccess.log to a Database

Using smauditimport data, you can push data from smaccess.log to a configured Database. Run this command to push the data:

```
Smauditimport  <full path of the file need to import>  <Data source name>  <Database user name> <Database password>
```

Add the SSO Reporting Tasks for PostgreSQL

1. Log in to the SiteMinder database as the SiteMinder database user.
2. Change directory to this location:

   ```
   /opt/jboss-eap-5.1.2/jboss-as/server/all/deploy/iam_im.ear/user_console.war/reports
   ```
3. Extract the ZIP file: cam-sso-postgresql-functions.zip
4. Run the following scripts as Identity Management Object Store Database User:

```
im-postgresql-audit_start_date.sql

im-postgresql-audit_end_date.sql
```

5. Change directory to JBoss/server/all/deploy/iam_im.ear/user-console.war/reports.
6. Copy the cam-sso-postgresql-reports.biar and cam-sso-oracle-reports.xml to the im_admin_tools_dir/ReportServerTools folder.
7. Rename cam-sso-oracle-reports.xml to cam-sso-postgres-reports.xml and replace all content with the following text:

```
<?xml version="1.0"?>
<biconfig version="1.0">
  <!-- Import BIAR file -->
  <step priority="1">
    <add>
                <biar-file
name="cam-sso-postgresql-reports.biar"/>
    </add>
  </step>
</biconfig>
```

8. Run the BIconfig utility to export cam-sso-postgresql-reports.biar into the Report Server.

```
./biconfig.sh -h "hostname" -u "administrator_name" -p
"administrator_password" -f "cam-sso-postgres-reports.xml"
```

Add the SSO Reporting Tasks for Oracle

1. Log in to SiteMinder database as the SiteMinder database user.
2. Run the following commands:

```
create or replace
FUNCTION IM_Audit_Start_Date (rangeVal int, multiplier int,
startdatetime DATE)

RETURN DATE is
tempid1 DATE;
BEGIN

if rangeVal = -1
then tempid1 := startdatetime;
else
case rangeVal
  when 1 then tempid1 := sysdate - multiplier;
--Last N days
  when 2 then tempid1 := trunc(sysdate, 'DAY') - (7 * multiplier);
--weekly
  when 3 then tempid1 := add_months(trunc(sysdate, 'month'),
-multiplier);
-- first day of the month
```

```
  when 4 then tempid1 := add_months(trunc(sysdate, 'month'), -(3
* multiplier));
-- quarter of the month
  when 5 then tempid1 := add_months(trunc(sysdate,'y'), -(12 *
multiplier));
--Yearly
  else tempid1 := sysdate;
end case;
end if;
return tempid1;
END;

create or replace
FUNCTION IM_Audit_End_Date (rangeVal int, enddatetime DATE)

RETURN DATE is
tempid1 DATE;
BEGIN
if rangeVal = -1
then tempid1 := enddatetime;
else
case rangeVal
  when 1 then tempid1 := sysdate;
--Last N days
  when 2 then tempid1 := trunc(sysdate, 'day') -1 + (1439/1440);
--weekly
  when 3 then tempid1 := trunc(sysdate, 'month') - 1 + (1439/1440);
-- last day of the month
  when 4 then tempid1 := trunc(sysdate, 'month') - 1 + (1439/1440);
-- quarter of the month
  when 5 then tempid1 := trunc(sysdate,'y')-1 + (1439/1440);
--Yearly
else tempid1 := sysdate;
end case;
end if;
return tempid1;
END;
```

Note: The previous commands are also found in the datefunctions.sql script. If you have access to this script, simply run the datefunctions.sql script file.

3. Change directory to *JBoss*/server/all/deploy/iam_im.ear/user-console.war/reports.
4. Copy the cam-sso-oracle-reports.biar and cam-sso-oracle-reports.xml to the *im_admin_tools_dir*/ReportServerTools folder.
5. Edit cam-sso-oracle-reports.xml and replace all content with the following text:

```
<?xml version="1.0"?>
<biconfig version="1.0">
  <!-- Import BIAR file -->
  <step priority="1">
```

```
    <add>
                <biar-file name="cam-sso-oracle-reports.biar"/>
    </add>
  </step>
</biconfig>
```

6. Run the BIconfig utility to export cam-sso-oracle-reports.biar into the Report Server.

```
./biconfig.sh -h "hostname" -u "administrator_name" -p
"administrator_password" -f "cam-sso-oracle-reports.xml"
```

Add JDBC Connections for Siteminder database

1. Log in to the User Console as the CSP administrator.
2. Add the JDBC tasks to the CSP Administrator role:
   a. In the left-hand navigation menu, select Roles and Tasks, Admin Roles, Modify Admin Role.
   b. Select CSP Administrator and click Select.
   c. Click the Tasks tab.
   d. Under Filter by Category, select System.
   e. Under Add Task, select Create JDBC Connection. Repeat to select Delete JDBC Connection, Modify JDBC Connection and View JDBC Connection.

      As you select each task, the task appears in the table of tasks that are assigned to the CSP Administrator role.
   f. Click Submit.
3. Make the JDBC tasks visible in the CSP Administrator's console:
   a. In the left-hand navigation menu, select Roles and Tasks, Admin Tasks, Modify Admin Task.
   b. Search for the string **JDBC**
   c. For each JDBC task, select the task, clear the Hide in Menus check box, and click Submit.

Enable the Single Sign On Manager Role

1. Log in to the User Console as the CSP administrator.
2. Select Roles and Tasks, Admin Roles, Enable/Disable Admin Role.
3. Enable the Single Sign On Manager role by selecting the check box, and click Select.
4. Click Yes to confirm.

   The system enables the Single Sign On Manager role.

Configure Reporting

The pre-configuration steps for SSO reports are complete. You now perform the steps in the Reporting Chapter of the *Identity Management Administration Guide*. The following procedure summarizes that chapter.

1. Configure a connection between the report server and Identity Management.
2. Create a JDBC connection object and specify the SiteMinder database connection details.
   a. Enter JDBC as the Connection Type.
   b. Under connection details, enter the SiteMinder audit database information and valid user credentials for a user who has access to the SiteMinder Audit DB. The SiteMinder audit database details can be found by running the smconsole utility.
3. Associate the JDBC connection with all SSO reports. Set the connection type as a JDBC Connection for the following SSO report tasks:
   - SSO-Authentications by Authentication Type Report
   - SSO-Unique User Authentications Detail Report
   - SSO-Unique User Authentications Summary Report
   - SSO-Authentications by Auth type per Application Report
   - SSO-User Accesses per Application Report
   - SSO-User Access Detail Report
   - SSO-User Authentication Detail Report

After you complete both pre-configuration and configuration steps for reporting, the tenant administrator can request SSO reports in the User Console.

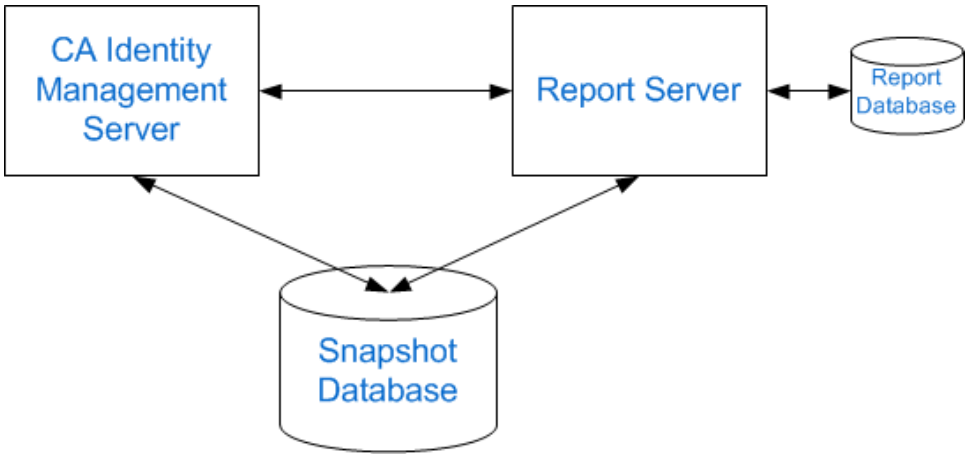
How to Create a Custom Report

Identity Management reports enable you to see the current state of a Identity Management environment. You can use this information to ensure compliance with internal business policies or external regulations.

You generate Identity Management reports from management data which describes the relationship between objects in Identity Management environment. Examples of management data include the following:

- Profile attributes of the users
- List of roles that contain a certain task
- The members of a role or group
- The rules that comprise a role

In Identity Management, the reporting setup requires the following three major components:



Note: The Snapshot Database in this illustration graphic could also be the Audit Database or Workflow Database.

Report Server

Also known as CA Business Intelligence, this server generates reports, communicating directly with Identity Management and the Snapshot Database.

Report Database

The database where the CA Report Server (Business Objects) stores its data.

CA Identity Management Server

CA Identity Management Server allows you to export Identity Management object data to the Report Database.

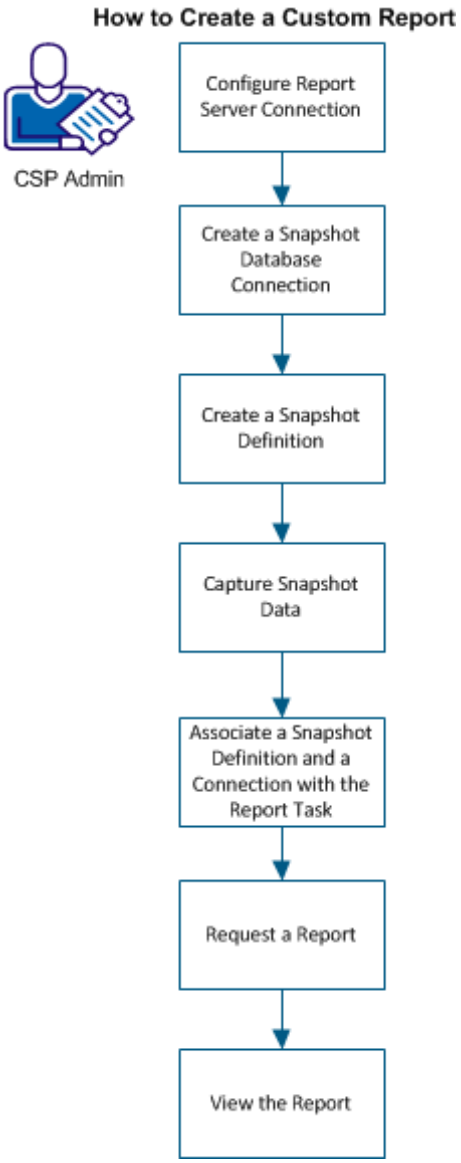
Snapshot Database

A separate database containing the snapshot data of objects in Identity Management

Important! The Report Server uses Business Objects Enterprise. If you already have a Report Server in your environment and want to use it with Identity Management, the minimum version required by Identity Management is CA Business Intelligence 3.2 SP5.

A snapshot report includes data from the Snapshot Database, which contains information from the Identity Management object store and the user store. An example of a snapshot report is the User Profile report. You define the snapshot data that is added to the Snapshot Database and using snapshot definitions, specify the information to include.

The following graphic illustrates the process for creating a custom report:



1. Configure the Report Server connection (see page 154).
2. Create a snapshot database connection (see page 155).
3. Create a Snapshot Definition (see page 156).
4. Capture the snapshot data (see page 157).
5. Associate a snapshot definition and a connection with the report task (see page 158).
6. Request a report (see page 159).
7. View the report (see page 160).

Configure the Report Server Connection

To collect data from the report server, you must configure the connection to the Report Server. Before you begin the procedure, gather the following information about the reporting server:

Name	Description
Host Name	The host name of the machine where the report server is installed
Port	The port name of the machine where the Report Server is installed
Reports folder name	The location of the default Identity Management reports.
User ID	Specifies the user created for the Report Server.
Password	Specifies the password for the user created in the Report Server.
Secure Connection	Specifies the security connection for the report server. Select the checkbox to enable Secure Sockets Layer (SSL) connection between Identity Management and Report Server. **Note**: Before you select the Secure Connection checkbox, verify that you have installed the certificate from the BOServer. For more information about how to configure SSL, see the Chapter "Report Server Installation" in the *Installation Guide*.
Web Server	Specifies the web server. Set to Non-IIS for Tomcat.

Note: We recommend that all systems involved in reporting be set to the same time zone and time.

Follow these steps:

1. In the User Console, click System, Reporting, Report Server Connection.
2. Enter the Report Server settings.
3. Click Test Connection to verify the connection.
4. Click Submit.

The reporting connection is established.

Create a Snapshot Database Connection

Create a snapshot database connection to the snapshot database in order to export snapshot data.

Follow these steps:

1. In the User Console, go to Reports, Snapshot Tasks, Manage Snapshot Database Connection, Create Snapshot Database Connection.
2. Create a new snapshot database connection by completing all the necessary fields.
3. Click Submit.

   A new Snapshot Database connection is created.

Create a Snapshot Definition

A snapshot reflects the state of objects in Identity Management at a given time. The snapshot data is used to build a report. To capture snapshot data, you create a snapshot definition that exports the data to the Snapshot Database. Using the snapshot definition, you define the rules to load users, endpoints, admin roles, provisioning roles, groups, and organizations.

Follow these steps:

1. In the User Console, go to Reports, Snapshot Tasks, Manage Snapshot Definition, Create Snapshot Definition.
2. Select Create or Copy an object of type Snapshot Type.
3. Click Ok.
4. Under the Profile tab, complete the following fields to create a snapshot definition profile:

   Snapshot Definition Name

   Identifies the unique name that is given for the snapshot definition.

   Snapshot Definition Description

   Displays any additional information that you want to describe the snapshot.

   Enabled

   Specifies that data is exported to the snapshot database at the scheduled time.

   Note: If this option is not selected, you cannot schedule to generate a snapshot report for this profile. Also, the snapshot definition is not listed in the Capture Snapshot Data screen.

   Number of snapshots retained

   Specifies the number of successful snapshots retained in the Snapshot Database.

   Note: If you do not specify a value for this field, Identity Management stores unlimited snapshots.
5. On the Snapshot Policies tab, select the objects that are related to the policies to export.
6. On the Role Settings tab, select one or more role components and available attributes for the snapshot to export.
7. On the User Attributes Details tab, select one or more user attributes for the snapshot to export.

   Note: In the Snapshot Policies tab, if you select only the User object, by default, all user attributes related data are exported.
8. On the Endpoint Account Attributes tab, select one or more account attributes for an endpoint type.

Note: For a selected endpoint type, by default, all data related to endpoint account attributes is exported. To capture data related to a specific attribute, select the appropriate attribute. For more information about selecting attributes that are necessary to export for an endpoint type, see the Default Reports section in the *Configuration Guide*.

9. (Optional) Select the Export Orphan Accounts check box to include endpoint accounts with no global user in the Provisioning Server.

   Note: To export report data for non-standard, non-standard-trend and orphan account reports, select exceptionAccount attribute and Export Orphan Accounts check boxes.

10. Click Submit.

    Identity Management is configured to create snapshots of the objects mentioned in the snapshot definition.

Now that you have created a snapshot definition, you can capture snapshot data immediately or can schedule the snapshot data export at a later time.

More information:

Recurrence Tab (see page 136)

Capture Snapshot Data

If you want to capture snapshot data immediately or schedule the snapshot data export at a later time or on a recurring schedule, run the Capture Snapshot Data task. This task exports the data (defined by the snapshot definition) to the Snapshot Database.

Important! Exporting snapshot data can take a long time if you have a large amount of data to export. We recommend you schedule your snapshots when exporting numerous data.

Follow these steps:

1. In the User Console, go to Reports, Snapshot Tasks, Capture Snapshot Data.
2. Select Execute now to run the data export immediately, or select Schedule new job (see page 136) to run the data export at a later time or on a recurring schedule.
3. Click Next.
4. Choose a snapshot definition.

5. Click Submit.

   Snapshot data is exported to the Snapshot Database.

Note: If the Capture Snapshot Data task seems to be taking a long time, you can check the progress of the task by going to the System tab and clicking View Submitted Tasks.

Associate a Snapshot Definition and a Connection with the Report Task

Assign a snapshot definition to a report task to specify the snapshot definition to be used when running the report.

Follow these steps:

1. In the User Console, go to Roles and Tasks, Admin Tasks, Modify Admin Task.
2. Search for the report task you want to associate a snapshot definition with.
3. Go to the Tabs tab and click Edit.
4. Click Add.
5. Search for the snapshot definition to associate with the report task and click Select.

   When associating a snapshot definition with a report task, note the following:

   - A report can be associated with one or more snapshot definitions.
   - A snapshot definition can be associated with more than one report.
   - Multiple snapshots associated with a single report task must not use the same recurrence time.
6. Click Ok.
7. Go to the Search tab and click Browse to locate the search screens.
8. Edit the search screen for the report task and choose rptParamConn under Connection Object for the Report, then click Ok.
9. Click Select.
10. Go to the Search tab and click Browse to locate the search screens.
11. Edit the search screen for the report task and choose the Snapshot Database Connection object.
12. Click Ok.
13. Click Submit.

The snapshot database definition and connection are now associated with the report task.

Request a Report

To view the report, request a report to a user with report administration privileges. Approval is required because some reports may require a long time or significant system resources to run. If your report request requires an approval, the system sends you an email alert.

Follow these steps:

1. Log in to the User Console with report tasks user privileges.
2. Select either:
   - Tasks, Reports
   - Reports
3. Select Reporting Tasks, and Request a Report.

   A list of reports appears.
4. Select the report that you want to request.

   A parameters screen appears.

   Provide any parameter information required.

   Note: If you are running a snapshot report and no snapshots are available for this report, you must first capture a snapshot.

   - Some reports show system status at a specific point in time. When you request this type of report, you select a point in time for which you want to see report data. This point in time is named a *snapshot*.

     Note: The snapshot dates and times you can choose are predetermined. Typically, your system administrator, or another user with report administration privileges, configures snapshots. If no snapshots are available for the report you want to request, contact a system administrator.
   - Some reports show activity over a time period. Titles for these reports usually begin with the word *Audit*. When you request this type of report, you specify a time period for which you want to see report data. For example, you can run the Audit-Reset Password report for the past 30 days.
5. Click Schedule Report, and select a schedule for your report.

   Now

   Specifies that the report runs immediately.

   Once

   Specifies that the report runs once, during a specific time period. Select the start date, end date, start time, and end time when you want to generate the report.

   Note: Consider selecting this option if the report you are requesting requires a large amount of data. To conserve system resources, choose a time when there is less system activity.

6. Click Submit.

   The report request is submitted. Depending on your environment configuration, the request runs immediately, or it runs after approval by an administrator.

   Typically, a system administrator or another user with report administration privileges must approve a report request before the system completes it. Approval is required because some reports can require a long time or significant system resources to run. If your report request requires approval, the system sends you an email alert.

View the Report

Depending on your environment configuration, a report will be available to view when an administrator approves the request for that report. If your report request is pending approval, the system sends you an email alert. The report that you want to view does not appear in the search list until it is approved.

Note: In order to view reports in Identity Management using the View My Reports task, enable third-party session cookies in your browser.

Follow these steps:

1. In the User Console, go to Reports, Reporting Tasks, and click View My Reports.
2. Search for the generated report that you want to view.

   Both recurrence generated reports and on-demand report instances are displayed.

   Note: If the status of the report is Pending/Recurring, the report is not generated and may take time to complete.
3. Select the report that you want to view.
4. (Optional) Click Export this report (top left corner) to export the report to the following formats:
   - Crystal Report
   - PDF
   - Microsoft Excel (97-2003)
   - Microsoft Excel (97-2003) Data-Only
   - Microsoft Excel (97-2003) - Editable
   - Rich Text Format (RTF)
   - Seperated Values (CSV)
   - XML

Running a Report

You can run reports for your CA CloudMinder environment. Generally, reports show either system status at a certain point, or system activity over a time period. For example, the Role Owners Report provides a current list of users who are role owners for each role in the system. The Audit-Reset Password Report shows password reset activity over a period you specify. CA CloudMinder includes many preconfigured reports that are designed to address common reporting needs.

Reports are used by various users. For example, a tenant administrator can run reports to gain information about the state of their environment and the activities of their users. A system administrator can run reports to facilitate configuration or maintenance tasks for a tenant environment. The following instructions use a tenant administrator as the example user, but any user with reporting privileges can follow the steps to generate and view reports.

Each report requires initial configuration before you can run it. Typically, your system administrator, or another user with report administration privileges, performs that configuration. Once initial configuration is complete, you can run the report.

Running a report is a two-step process unless the report can be run in 15 seconds. In that case, you use one task to request and view the report. Otherwise, when you request a report, the system gathers and processes the required data. After you request a report, you can view it.

How to Request and View a Snapshot Report

Snapshot reports enable you to see the current state of a Identity Management environment. You can use this information to ensure compliance with internal business policies or external regulations.

You can generate snapshot reports from management data which describes the relationship between objects in Identity Management environment. Examples of management data include the following:

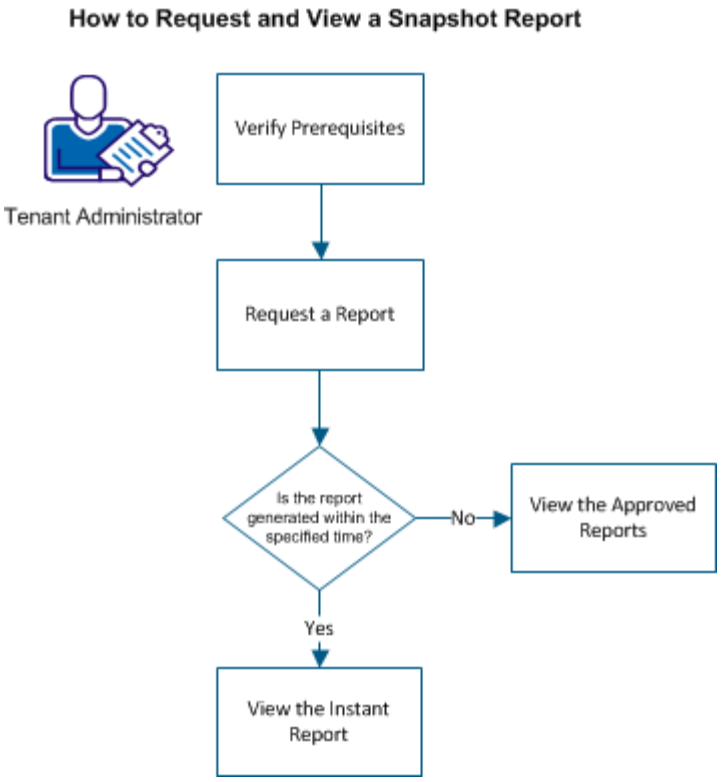
- Profile attributes of the users
- List of roles that contain a certain task
- The members of a role or group
- The rules that comprise a role

A snapshot report include data from the Snapshot Database, which contains information from the Identity Management object store and the user store. Depending upon the report type, your request to view a report is taken immediately or is sent for approval to the CSP administrator.

The following is a list of default snapshot reports available in Identity Management:

- Account Details Report
- Administration Report
- Billing Report
- Endpoint Accounts Report
- Endpoint Details Report
- Non-Standard Accounts Report
- Non-Standard Accounts Trend Report
- Orphan Accounts Report
- Role Administrators Report
- Role Members Report
- Role Owners Report
- Roles Report
- Snapshots Report
- Task Roles Report
- User Accounts Report
- User Entitlements Report
- User Profile Report
- User Roles Report

The following graphic illustrates the process to request and view a snapshot report:



To run the snapshot report, perform the following steps:

1. Verify prerequisites (see page 163)
2. Request and view a report (see page 164)
3. Depending on the time taken for the report to generate, do one of the following steps:
   - View the instant report (see page 165)
   - View the approved reports (see page 165)

Verify Prerequisites

As a Tenant administrator, if you are requesting a report for the first time, contact the CSP administrator to verify that the snapshot is captured for the report.

Request and View a Report

To view a report, select one of the assigned default reports. Your request for report is sent to the hosting administrator for approval or the report is generated immediately. If your report request requires an approval, the system sends you an email alert. Upon approval, the system generates the latest snapshot to view the report.

Note: Although an Identity Policy appears in the snapshot definition screens, this policy is not used when the reports are generated. Identity Policies are not a feature of CA CloudMinder.

Follow these steps:

1. Log in to the User Console with reporting privileges.
2. Select Reports, Reporting Tasks, and Request & View a Report.

   A list of reports appears.
3. Select the report name that you want to request.

   A parameter screen appears.

   Note: If you are requesting for a Non-Standard Accounts Trend Report, contact the CSP administrator to capture a snapshot.
4. Select the Snapshot Time or Report ID

   Snapshot Time or Report ID

   Specifies the latest snapshot instance that is used to generate the report. If you want to view a report of existing snapshot data, the snapshot time and date of an earlier snapshot data is created. For example, if the hosting administrator sets the snapshot capture time for every hour, your second request after the given time interval creates a snapshot date and time to view the old snapshot data.
5. Select the other report parameters.

   Note: Select the wild-card (*) to include all the parameters in the list.
6. Click Generate Report.

   The system waits for the process to begin and confirms the status of the report. If the report generation takes long time, a message appears with the instructions on how to view the requested report later. If the reports are configured with an e-mail notification, the system sends an e-mail to the administrator for the approval. Upon approval, you receive an e-mail with a message of task completion.
7. Click Submit.

   The report request is submitted.

Note: If you plan to generate and view the reports periodically, use Schedule Reports.

View the Instant Report

Depending on the environment configuration, the report is generated immediately or a message appears with the instructions on how to view the requested report later. If the report runs immediately within the specified time of the report, the screen is refreshed and the generated report is displayed.

Click Export this report (top left corner) to export the report data to the following formats:

- Crystal Report
- Excel
- PDF

View the Approved Reports

A report will be available to view when an administrator approves the request for that report. If your report request is in pending for approval, the system sends you an email alert. The report that you want to view does not appear in the search list until it is approved.

Follow these steps:

1. In the User Console, go to Reports, Reporting Tasks, and click View My Reports.
2. Search for the report you want to view.

   Both recurrence reports and on-demand report instances are displayed.
3. Select the report that you want to view.

   Note: In order to view reports in Identity Management using the View My Reports task, enable third-party session cookies in your browser.
4. (Optional) Click Export this report (top left corner) to export the report to the following formats:
   - Crystal Report
   - Excel
   - PDF

How to Request and View an Audit Report

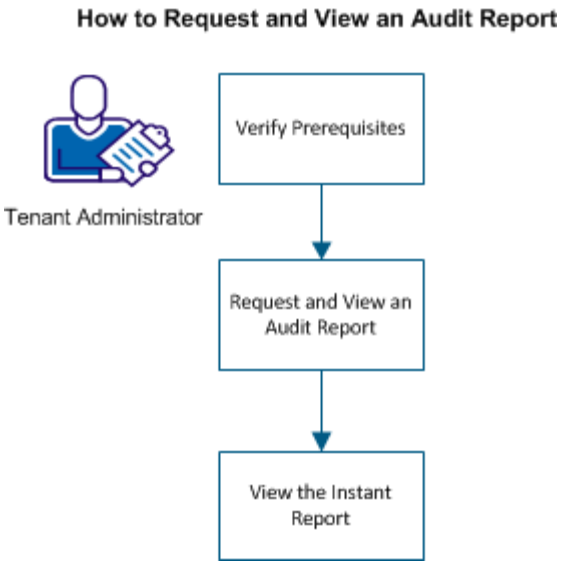
An audit report provides a historical record of operations that occur in an environment. Some examples of audit data include the following points:

- System activity for a specified period of a time
- User login and logout events while accessing a particular environment
- The tasks that a specific user performs
- A list of objects that were modified during a specific period of a time.
- The user assigned roles
- The operations which are performed for a particular user account.

The following is a list of default audit reports:

- Assign Revoke Provisioning Roles Report
- De-Provisioning Report
- Audit Details Report
- Pending Approval Tasks Report
- Reset Password Report
- Tasks Performed by Administrator

The following graphic illustrates the process to request and view an audit report:



To run the audit report, perform the following steps:

1. Request and view an audit report (see page 167).

2. Depending on the time taken for the report to generate, do one of the following steps:
   - View the instant report (see page 165).

Request and View an Audit Report

To view a report, select one of the assigned default reports in the user console.

Follow these steps:

1. Log in to the User Console with reporting privileges.
2. Select Reports, Reporting Tasks, and Request & View a Report.

   A list of reports appears.
3. Select the report that you want to request.
4. Click Next.

   A parameter screen appears.
5. Provide the Start Date Time and End Date Time in *M/d/yyyy H:mm* format.
6. Click Generate Report.

   The system waits for the process to begin and confirms the status of the report. If the selected report is configured with an e-mail notification, you receive an e-mail when the task completes.
7. Click Submit.

   The report request is submitted. Depending on your environment configuration, you can view the report immediately or you can view it from the *View My Reports* section.

Note: If you plan to generate and view the reports periodically, use Schedule Reports.

View the Instant Report

Depending on the environment configuration, the report is generated immediately or a message appears with the instructions on how to view the requested report later. If the report runs immediately within the specified time of the report, the screen is refreshed and the generated report is displayed.

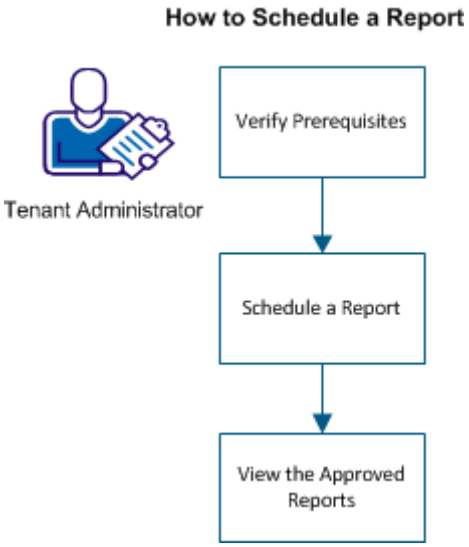
Click Export this report (top left corner) to export the report data to the following formats:

- Crystal Report
- Excel
- PDF

How to Schedule a Report

Some reports may take a long time to run, or you may want to view the same report multiple times without re-running the report each time you view it. Scheduling a report allows you to schedule the automatic generation of a report to occur at a later time. Once the report is generated, you can view the report multiple times without re-running the report.

The following graphic illustrates the process on how to schedule a report:



To run the snapshot report, perform the following steps:

1. Verify prerequisites (see page 163)
2. Schedule a report (see page 169)
3. View the approved reports (see page 165)

Verify Prerequisites

As a Tenant administrator, if you are requesting a report for the first time, contact the CSP administrator to verify that the snapshot is captured for the report.

Schedule a Report

You can plan to generate and view a report periodically, based upon your business needs. To schedule a report, select any default report and specify the schedule parameters for the selected report.

Follow these steps:

1. Log in to the User Console with reporting privileges.
2. Select Reports, Reporting Tasks, and Request & View a Report.

   A list of reports appears.
3. Select the report that you want to request.

   A parameter screen appears.

   Note: If you are requesting for a Non-Standard Accounts Trend Report, contact the Tenant or CSP administrator to capture a snapshot.
4. Select the Snapshot Time or Report ID

   Snapshot Time or Report ID

   Specifies the latest snapshot instance that is used to generate the report. If you want to view a report of existing snapshot data, a Report ID for the earlier snapshot data is created. For example, if the hosting administrator sets the snapshot capture time for every hour, your second request after the given time interval creates a Report ID to view the old snapshot data.
5. Select the other report parameters.

   Note: Select the wildcard (*) to include all the parameters in the list.
6. For a Non-Snapshot related report such as *Audit details*, specify the time in numeric value. For example, if you want to schedule report for every two weeks, specify as *2* in the field.
7. Click Schedule new job.

   Parameters related to scheduling appears.
8. Enter the following values:

   Job Name

   Specifies the name of the job you want to create or modify.

   Time Zone

   Specifies the server time zone.

   Note: If your time zone is different from the server's time zone, a drop-down box is displayed so you can select either your time zone or the server's time zone when scheduling a new job. You cannot change the time zone when modifying an existing job.

Daily schedule

Specifies that the job runs every certain number of days.

Every (number of days)

Defines the number of days between that the job runs.

Weekly schedule

Specifies that the job runs on a specific day or days and time during a week.

Day of Week

Specifies the day or days of the week that the job runs.

Monthly schedule

Specifies a day of week or day of month that the job runs on a monthly basis.

Yearly schedule

Specifies a day of week or day of month that the job runs on a yearly basis.

Advanced schedule

Specifies additional scheduling information.

Cron Expression

For information about filling out this field, go to the following website*:*

http://quartz-scheduler.org/api/2.1.0/org/quartz/CronExpression.html

Execution Time

Specifies the time of day, in 24-hour format, that the job is run. For example, 14:15.

9. Click Submit.

The system confirms the report schedule. If the selected report is configured with an e-mail notification, an e-mail is sent when the task completes.

View the Approved Reports

A report will be available to view when an administrator approves the request for that report. If your report request is in pending for approval, the system sends you an email alert. The report that you want to view does not appear in the search list until it is approved.

Follow these steps:

1. In the User Console, go to Reports, Reporting Tasks, and click View My Reports.
2. Search for the report you want to view.

   Both recurrence reports and on-demand report instances are displayed.
3. Select the report that you want to view.

   Note: In order to view reports in Identity Management using the View My Reports task, enable third-party session cookies in your browser.
4. (Optional) Click Export this report (top left corner) to export the report to the following formats:
   - Crystal Report
   - Excel
   - PDF

Troubleshooting

When viewing a report in Identity Management, you may be re-directed to the Business Objects Infoview login page.

Follow these steps:

1. Right-click on the Infoview login web page and select View Source.
2. Find the URL for the report.
3. Copy and paste the URL into a new browser window.
4. If you do not see the report, contact a system administrator.
5. If you do see the report, try the following to fix the browser settings:
   - Accept third-party cookies.
   - Allow session cookies.
   - Remove High security settings.

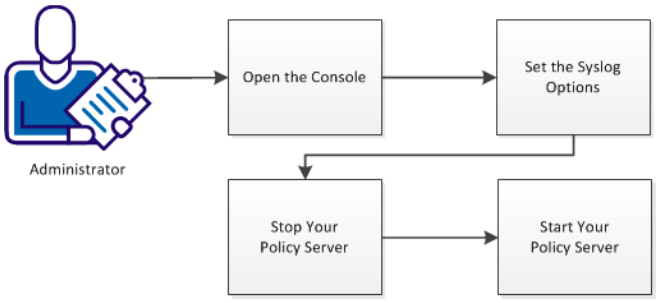
Chapter 8: Monitoring

This section contains the following topics:

How to Record Events to the Syslog

Administrators can record Policy Server events to the syslog on supported operating environments. The following graphic describes how to record events to the syslog:

How to Record Events to the Syslog



Follow these steps:

1. Open the console (see page 174).
2. Set the syslog options (see page 174).
3. Restart your Policy Server with the following steps:
   - Stop your Policy Server (see page 177).
   - Start your Policy Server (see page 177).

Open the Console

To change your settings, open the console.

Follow these steps:

1. Verify that an X-windows server is running on your system.
2. Open a terminal window.
3. Set the DISPLAY variable with the following command:

   ```
   export DISPLAY=IP_address:0.0
   ```

   IP_address

   Specifies the IP address of where the console window appears. Use the IP address of the system from which you are *connecting to* the console.

   Example: (IPV4) 192.168.1.1

   Example: (IPV6) 2001:DB8::/32
4. Log in to the system hosting the console.
5. Navigate to the following directory:

   ```
   installation_directory/siteminder/bin
   ```

   installation_directory

   Specifies the location in the file system where the Policy Server is installed.

   Default: /opt/CA/siteminder
6. Open the console by running the following command:

   ```
   ./smconsole
   ```

Set the Syslog Options

Setting the syslog options on the console specifies which events are recorded in the syslog.

Note: For more information about the Syslog and its settings, see this website.

Follow these steps:

1. Enable syslog recording with the following steps:
   a. Click the Data tab.
   b. Click the Database drop-down list, and then pick Audit Logs.
   c. Click the Storage drop-down list, and then pick Syslog.

2. Select the text in the Priority field, and then type the value that you want from the following list:

   Priority

   Specifies the event priority recorded in the syslog. Pick *one* of the following values:

   - LOG_EMERG
   - LOG_ALERT
   - LOG_CRIT
   - LOG_ERR
   - LOG_WARNING
   - LOG_NOTICE
   - LOG_INFO
   - LOG_DEBUG

   Default: LOG_INFO

3. Select the text in the Facility field, and then type value that you want from the following list:

   Facility

   Specifies which events in the operating environment are recorded to the syslog. Pick *one* of the following values:

   - LOG_AUTH
   - LOG_AUTHPRI
   - LOG_CRON
   - LOG_DAEMON
   - LOG_FTP
   - LOG_KERN
   - LOG_LPR
   - LOG_MAIL
   - LOG_NEWS
   - LOG_SYSLOG
   - LOG_USER
   - LOG_UUCP
   - LOG_LOCAL0
   - LOG_LOCAL1
   - LOG_LOCAL2
   - LOG_LOCAL3
   - LOG_LOCAL4
   - LOG_LOCAL5
   - LOG_LOCAL6
   - LOG_LOCAL7

   Default: LOG_AUTH

4. (Optional) Replace the text in the following field:

   Text

   Specifies the text in an event that you want to record in the syslog. For example, if you specify the word tiger, then any events containing the word tiger are recorded in the syslog.

   Default: Siteminder

5. Click OK.

   The console closes and the syslog options are set.

Stop a UNIX Policy Server

Stopping a Policy Server has the following results:

- The Policy Server is temporarily removed from your environment.
- Agents who need authorization or authentication decisions cannot contact the stopped Policy Server. Those Agents can still connect to other Policy Servers that are available.
- All logging activity stops.

Follow these steps:

1. Log in to the system hosting the Policy Server with the same user account that installed the Policy Server originally.
2. Stop all Policy Server processes, with *one* of the following actions:
   - Open the Management Console, click the Status tab, and then click the Stop buttons.
   - Use the following script. This script also stops the UNIX executive so that the processes do not restart automatically.

     ```
     installation_path/siteminder/stop-all
     ```

     The Policy Server logs all UNIX executive activity in the installation_directory/log/smexec.log file. Log entries are always appended to the existing log file.

Start a UNIX Policy Server

Starting Policy Server has the following results:

- Agents contact the Policy Server for authorization or authentication decisions.
- Logging begins.

Start all Policy Server processes, with *one* of the following actions:

- Open the Management Console, click the Status tab, and then click the Start buttons.
- Use the following script. This script also starts the UNIX executive.

  ```
  installation_path/siteminder/start-all
  ```

  The Policy Server logs all UNIX executive activity in the installation_directory/log/smexec.log file. Log entries are always appended to the existing log file.

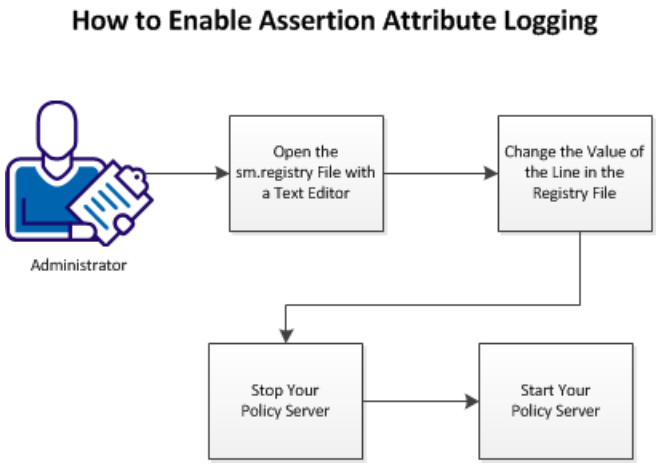
How to Enable Assertion Attribute Logging on UNIX or Linux Operating Environments

You can record information about the assertion attributes to the audit logs. Use these logs for a security audit, or during an investigation. The type of event determines the information that is recorded in the log. The following events are recorded when you enable assertion-attribute logging:

- Any assertion generations
- Any assertion consumptions
- Any authentication success
- Any authentication failures
- Any authentication attempts
- Any application access

The logging of assertion attributes is disabled by default. Enable assertion-attribute logging on your Policy Server.

The following graphic describes how to enable assertion-attribute logging:



Follow these steps:

1. Open the sm.registry file with a text editor (see page 179).
2. Change the value of the line in the registry file (see page 180).
3. Restart your Policy Server with the following steps:
   a. Stop your Policy Server (see page 177).
   b. Start your Policy Server. (see page 177)

Open the sm.registry File with a Text Editor

Change this setting on UNIX or Linux operating environments by opening the sm.registry file with a text editor. The sm.registry file is stored on your Policy Server.

Follow these steps:

1. Navigate to the following directory:

   Installation_Directory/registry

   installation_directory

   Specifies the location in the file system where the Policy Server is installed.

   Default: /opt/CA/siteminder

2. Open the following file with a text editor:

   sm.registry

   You can now change the settings.

Change the Value of the Line in the Registry File

The following entry in the sm.registry file controls attribute assertion logging:

Enable Enhance Tracing

Indicates whether attribute assertions are recorded in the audit logs. A value of 2 enables logging. A value of 3 enables logging and records the authentication method of the user.

Limits: 0, 2, 3

Default: 0 (logging disabled)

Follow these steps:

1. Locate the following section of the sm.registry file:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\Reports=
   ```

2. Locate the following line in the Reports section:

   ```
   Enable Enhance Tracing=      0; REG_DWORD
   ```

3. Change the zero to *one* of the following values:
   - 2 (enables logging)
   - 3 (enables logging and records the authentication method)

4. Verify that the line in your sm.registry file matches *one* of the following examples:

   ```
   Enable Enhance Tracing=      2; REG_DWORD
   ```

   ```
   Enable Enhance Tracing=      3; REG_DWORD
   ```

5. Save the changes to the sm.registry file, and then close the text editor.

   The value of the line in the registry file is changed.

Stop a UNIX Policy Server

Stopping a Policy Server has the following results:

- The Policy Server is temporarily removed from your environment.
- Agents who need authorization or authentication decisions cannot contact the stopped Policy Server. Those Agents can still connect to other Policy Servers that are available.
- All logging activity stops.

Follow these steps:

1. Log in to the system hosting the Policy Server with the same user account that installed the Policy Server originally.
2. Stop all Policy Server processes, with *one* of the following actions:
   - Open the Management Console, click the Status tab, and then click the Stop buttons.
   - Use the following script. This script also stops the UNIX executive so that the processes do not restart automatically.

     ```
     installation_path/siteminder/stop-all
     ```

     The Policy Server logs all UNIX executive activity in the installation_directory/log/smexec.log file. Log entries are always appended to the existing log file.

Start a UNIX Policy Server

Starting Policy Server has the following results:

- Agents contact the Policy Server for authorization or authentication decisions.
- Logging begins.

Start all Policy Server processes, with *one* of the following actions:

- Open the Management Console, click the Status tab, and then click the Start buttons.
- Use the following script. This script also starts the UNIX executive.

  ```
  installation_path/siteminder/start-all
  ```

  The Policy Server logs all UNIX executive activity in the installation_directory/log/smexec.log file. Log entries are always appended to the existing log file.