Manage Users

About user profiles

A user profile defines the login, password, email, and role (permissions) of a user.

You can configure both internal and external profiles for users. Internal user profiles reside in Catalyst Center, and external user profiles reside on an external AAA server.

A default user profile with SUPER-ADMIN-ROLE permissions is created when you install Catalyst Center.

About user roles

Users are assigned user roles that specify the functions that they are permitted to perform:

- **Administrator (SUPER-ADMIN-ROLE)**: Users with this role have full access to all of the Catalyst Center functions. They can create other user profiles with various roles, including those with the SUPER-ADMIN-ROLE.

- **Network Administrator (NETWORK-ADMIN-ROLE)**: Users with this role have full access to all of the network-related Catalyst Center functions. However, they do not have access to system-related functions, such as backup and restore.
- **Observer (OBSERVER-ROLE)**: Users with this role have view-only access to the Catalyst Center functions. Users with an observer role cannot access any functions that configure or control Catalyst Center or the devices it manages.
- **Customized Role**: User with SUPER-ADMIN-ROLE privileges can define custom roles that permit or restrict user access to certain Catalyst Center functions.

Create an internal user

You can create a user and assign this user a role.

Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see About user roles, on page 1.

Procedure

Step 1 From the main menu, choose **System** > **Users & Roles** > **User Management**.

Step 2 Click **Add**.

Step 3 Enter a first name, last name, email address, and username for the new user.

The email address must meet the requirements for the standard Apache EmailValidator class.

Step 4 Under **Role List**, choose one of the following roles: **SUPER-ADMIN-ROLE**, **NETWORK-ADMIN-ROLE**, or **OBSERVER-ROLE**.

Step 5 Enter a password and confirm it.

Step 6 Click **Save**.

Edit a user

You can edit some user properties (but not the username).

Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see About user roles, on page 1.

Procedure

Step 1 From the main menu, choose **System** > **Users & Roles** > **User Management**.

Step 2 Click the radio button next to the user that you want to edit.

Step 3 Click **Edit**.

Step 4 Edit the first or last name or email address, if needed.

Step 5 Under **Role List**, choose a new role, if needed: **SUPER-ADMIN-ROLE**, **NETWORK-ADMIN-ROLE**, or **OBSERVER-ROLE**.

Step 6 Click **Save**.

Delete a user

Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see About user roles, on page 1.

Procedure

Step 1 From the main menu, choose **System** > **Users & Roles** > **User Management**.

Step 2 Click the radio button next to the user that you want to delete.

Step 3 Click **Delete**.

Step 4 At the confirmation prompt, click **Continue**.

Password policy

After you have deployed Catalyst Center, keep these points regarding password policy in mind:

Fresh Catalyst Center deployments

- The default password for the maglev user and admin superuser is **P@ssword9**.

  You are prompted to change the admin superuser's password after you log in to the Catalyst Center GUI for the first time.

- When you change any user's password, or configure a new user, their password must comply with the new requirements.

Catalyst Center upgrades

- RBAC users configured in an earlier version of Catalyst Center can continue using their current password to log in to Catalyst Center 2.3.7.9 and later.

  For example, say you upgraded an appliance from version 2.3.7.6 to 2.3.7.9. Then you backed up this appliance's data. And later, you restored its backup file onto another appliance that has Catalyst Center 2.3.7.9 installed. Existing RBAC users will be able to log in using their current password.

- When you change any user's password, or configure a new RBAC user, their password must comply with the new requirements.

See Password requirements, on page 4 for a description of the criteria that newly created user passwords must meet.

Password requirements

Any user password you configure in Catalyst Center 2.3.7.9 or later must meet these requirements:

- It is at least nine characters in length.
- It contains characters from at least three of these categories:
  - Uppercase letters (A–Z)
  - Lowercase letters (a–z)
  - Numbers (0 through 9)
  - Special characters (such as !, $, and #)
- It doesn't use more than four consecutive characters on an English QWERTY keyboard.

  For example, `59Asdfpj!` is not a valid password because it contains the characters `a`, `s`, `d`, and `f` in succession.
- It doesn't contain two or more consecutive characters from the associated username.
- It doesn't contain a complete word found in any language or a phrase that's based on personal information.

Note You can reuse a previous password only after 24 different passwords have been used.

Reset a user password

You can reset another user's password.

For security reasons, passwords are not displayed to any user, not even to the users with administrator privileges.

Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see About user roles, on page 1.

Procedure

Step 1 From the main menu, choose **System** > **Users & Roles** > **User Management**.
Step 2 Click the radio button next to the user whose password you want to reset.
Step 3 From the **More Actions** drop-down list, click **Reset Password**.
Step 4 Enter a new password and confirm it.
Step 5 Click **Save**.

Change your own user password

Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see About User Roles.

Procedure

Step 1 From the main menu, choose **System** > **Users & Roles** > **Change Password**.
Step 2 Enter information in the required fields.
Step 3 Click **Update**.

Change your own user password without admin permission

The following procedure describes how to change your password without admin permission.

Procedure

Step 1 From the top-right corner, click your displayed username and choose **My Profile and Settings** > **My Account**.
Step 2 In the **Password** field, click **Update Password**.
Step 3 In the **Update Password** dialog box, enter the new password and confirm the new password.
Step 4 Click **Update**.

Reset a forgotten password

If you forgot your password, you can reset it through the CLI.

Procedure

Step 1 Enter this command to check if the user is created in the system.

```
magctl user display <username>
```

The command returns the tenant-name, which can be used to reset the password. The output looks similar to:

```
User admin present in tenant TNT0 (where TNT0 is the tenant-name)
```

Step 2 Enter this command and the tenant-name to reset the password.

```
magctl user password update <username> <tenant-name>
```

You are prompted to enter a new password.

Step 3 Enter the new password.

You are prompted to reenter the new password to confirm.

Step 4 Enter the new password.

The password is reset, and you can log in to Catalyst Center using the new password.

Configure role-based access control

Catalyst Center supports role-based access control (RBAC), which enables a user with SUPER-ADMIN-ROLE privileges to define custom roles that permit or restrict user access to certain Catalyst Center functions.

Use this procedure to define a custom role and then assign a user to that role.

Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure.

Procedure

Step 1 Define a custom role.

a) From the main menu, choose **System** > **Users & Roles** > **Role Based Access Control**.
b) Click **Create a New Role**.
c) If a task overview window opens, click **Let's do it** to go directly to the workflow.
d) In the **Create a New Role** window, enter a name for the role and then click **Next**.

e) In the **Define the Access** window, click the **>** icon corresponding to the desired function to view the associated features.
f) Set the permission level to **Deny**, **Read**, or **Write** for the desired features and click **Next**.

   If you set the permission level of a feature to **Deny**, the user to whom you assign this role cannot view this feature in the GUI.

   For dependent features, if you override the recommended permission level settings, a warning message indicating the permission level violation of dependent features is shown in the **Summary** window.

g) Review the configuration settings. To make any changes, click **Edit**.
h) Click **Create Role**.

Step 2 To assign a user to the custom role you created, go to **Users & Roles** > **User Management**.

- To assign the custom role to an existing user:
  a. In the **User Management** window, click the radio button corresponding to the user to whom you want to assign the custom role, and then click **Edit**.
  b. In the **Update Internal User** slide-in pane, click the **Roles** drop-down list and choose the custom role.
  c. Click **Save**.
- To assign the custom role to a new user:
  a. In the **User Management** window, click **Add**.
  b. In the **Create Internal User** slide-in pane, enter the first name, last name, and username.
  c. From the **Roles** drop-down list, choose the custom role.
  d. Enter the password and then confirm it.
  e. Click **Save**.

Step 3 If you are an existing user who was logged in when the administrator was updating your access permissions, you must log out of Catalyst Center and then log back in for the new permission settings to take effect.

Catalyst Center user role permissions

Table 1: Catalyst Center user role permissions

Capability	Description
Assurance	Assure consistent service levels with complete visibility across all aspects of your network.

Capability	Description
Monitoring and Troubleshooting	Monitor and manage the health of your network with issue troubleshooting and remediation, proactive network monitoring, and insights driven by AI Network Analytics. This role lets you: • Resolve, close, and ignore issues. • Run Machine Reasoning Engine (MRE) workflows. • Analyze trends and insights. • Troubleshoot issues, including path trace, sensor dashboards, and rogue management. • Run workflows for rogue and Cisco Advanced Wireless Intrusion Prevention System (aWIPS). These workflows include AP-allowed list, vendor-allowed list, aWIPS profile creation, assigning an aWIPS profile, and so on.
Monitoring Settings	Configure and manage issues. Update network, client, and application health thresholds. Note: You must have at least Read permission on **Monitoring and Troubleshooting**.
Troubleshooting Tools	Create and manage sensor tests. Schedule on-demand forensic packet captures (Intelligent Capture) for troubleshooting clients. Note: You must have at least Read permission on **Monitoring and Troubleshooting**.
Network Analytics	Manage network analytics-related components.
Data Access	Enable access to query engine APIs. Control functions such as global search, rogue management, and aWIPS. Note: Setting the permission to Deny affects Search and Assurance functionality.
Network Design	Set up the network hierarchy, update your software image repository, and configure network profiles and settings for managing your sites and network devices.
Advanced Network Settings	• Update network settings, such as global device credentials, authentication and policy servers, certificates, trusted certificates, cloud access keys, Stealthwatch, Umbrella, and data anonymization. • Export the device inventory and its credentials. Note: To complete this task, you must have Write permission on **Network Settings**.
Image Repository	Manage software images and facilitate upgrades and updates on physical and virtual network entities.
Network Hierarchy	Define and create a network hierarchy of sites, buildings, floors, and areas based on geographic location. Users with this role can also add CMX servers in **System** > **Settings**.
Network Profiles	Create network profiles for routing, switching, and wireless. Assign profiles to sites. This role includes CLI Templates, Tagging, Feature Templates, and Authentication Template. Note: To create SSIDs, you must have Write permission on **Network Settings**.

Capability	Description
Network Settings	Common site-wide network settings such as AAA, NTP, DHCP, DNS, Syslog, SNMP, and Telemetry. Users with this role can add an SFTP server and modify the Network Resync Interval in **System** > **Settings**. Note: To create wireless profiles, you must have Write permission on **Network Profiles**. To assign a CMX server to a site, building, or floor, you must have Write permission on **Network Hierarchy**.
Virtual Network	Manage virtual networks (VNs). Segment physical networks into multiple logical networks for traffic isolation and controlled inter-VN communication.
Network Provision	Configure, upgrade, provision, and manage your network devices.
Compliance	Manage compliance provisioning.
EoX	Scan the network for details on publicly announced information pertaining to the **End of Life**, **End of Sales**, or **End of Support** of the hardware and software in your network. Note: To view EoX scans, you must have Read permission on **Compliance**. To run EoX scans, you must have Write permission on **Compliance**.
Image Update	Upgrade software images on devices that don't match the Golden Image settings after a complete upgrade lifecycle.
Inventory Management	Discover, add, replace, or delete devices on your network while managing device attributes and configuration properties. Note: To replace a device, you must have Write permission on **Network Provision** > **PnP**.
Inventory Management > Device Configuration	Device Configuration: Display the running configuration of a device.
Inventory Management > Discovery	Discovery: Discover new devices in your network.
Inventory Management > Network Device	Network Device: Add devices from Inventory, view device details, and perform device-level actions.
	Inventory Insights: Displays device issues, such as Speed/Duplex settings mismatch and VLAN mismatch, and the number of times each issue occurred. Provides detailed actions for users to perform to revolve the issues. Because this information requires action, including possible configuration changes, it is not displayed to users who have a read-only role.
Inventory Management > Port Management	Port Management: Allow port actions on a device.
Inventory Management > Topology	Topology: Display network device and link connectivity. Manage device roles, tag devices, customize the display, and save custom topology layouts. Note: To view the SD-Access Fabric window, you must have at least Read permission on **Network Provision** > **Inventory Management** > **Topology**.
License	Unified view of your software and network assets relative to license usage and compliance. The role also controls permissions for cisco.com, Cisco credentials, device EULA, and Smart accounts.

Capability	Description
Network Telemetry	Enable or disable the collection of application telemetry from devices. Deploy related settings, such as site telemetry receivers, wireless service assurance, and controller certificates, to devices. Note: To enable or disable the collection of application telemetry, you must have Write permission on **Provision**.
PnP	Automatically onboard new devices, assign them to sites, and configure them with site-specific contextual settings.
Provision	Provision devices with the site-specific settings and policies that are configured for the network. This role includes Fabric, Application Policy, Application Visibility, Cloud, Site-to-Site VPN, Network/Application Telemetry, Stealthwatch, Sync Start vs Run Configuration, and Umbrella provisioning. On the main dashboards for rogue and aWIPS, you can enable or disable certain actions, including rogue containment. To provision devices, you must have Write permission on **Network Design** and **Network Provision**.
Network Services	Configure additional capabilities on the network beyond basic network connectivity and access.
Application Hosting	Deploy, manage, and monitor virtualized and container-based applications running on network devices.
Bonjour	Enable the Wide Area Bonjour service across your network to enable policy-based service discovery.
Stealthwatch	Configure network elements to send data to Cisco Stealthwatch to detect and mitigate threats, even in encrypted traffic. To provision Stealthwatch, you must have Write permission on the following components: • **Network Design** > **Network Settings** • **Network Provision** > **Provision** • **Network Services** > **Stealthwatch** • **Network Design** > **Advanced Settings**

Capability	Description
Umbrella	Configure network elements to use Cisco Umbrella as the first line of defense against cybersecurity threats. To provision Umbrella, you must have Write permission on the following components: • **Network Design** > **Network Settings** • **Network Provision** > **Provision** • **Network Provision** > **Scheduler** • **Network Services** > **Umbrella** You must also have Read permission on **Advanced Network Settings**.
Platform	Open platform for accessible, intent-based workflows, data exchange, notifications, integration settings, and third-party app integrations.
APIs	Drive value by accessing Catalyst Center through REST APIs.
Bundles	Enhance productivity by configuring and activating preconfigured bundles for ITSM integration.
Events	Subscribe to get notified in near real time about network and system events of interest and initiate corrective actions. You can configure email and syslog logs in **System** > **Settings** > **Destinations**.
Reports	Generate reports using predefined reporting templates for all aspects of your network. Generate reports for rogue devices and for aWIPS. You can configure webhooks in **System** > **Settings** > **Destinations**.
Security	Manage and control secure access to the network.
Group-Based Policy	Manage group-based policies for networks that enforce segmentation and access control based on Cisco security group tags. This role includes Endpoint Analytics.
IP-Based Access Control	Manage IP-based access control lists that enforce network segmentation based on IP addresses.
Security Advisories	Scan the network for security advisories. Review and understand the impact of published Cisco security advisories that may affect your network.
System	Centralized administration of Catalyst Center, which includes configuration management, network connectivity, software upgrades, and more.
Machine Reasoning	Configure automatic updates to the machine reasoning knowledge base to rapidly identify security vulnerabilities and improve automated issue analysis.
System Management	Manage core system functionality and connectivity settings. Manage user roles and configure external authentication. This role includes Integrity Verification, HA, Disaster Recovery, Debugging Logs, Product Telemetry, System EULA, IPAM, Cisco AI Analytics, Backup & Restore, and Data Platform.

Capability	Description
Utilities	One-stop-shop productivity resource for the most commonly used troubleshooting tools and services.
Audit Log	Detailed log of changes made via UI or API interface to network devices or Catalyst Center.
Event Viewer	View network device and client events for troubleshooting.
Network Reasoner	Initiate logical and automated troubleshooting for network issues while drawing on the knowledge wealth of network domain experts.
Remote Device Support	Allow the Cisco support team to remotely troubleshoot the network devices managed by Catalyst Center. With this role enabled, an engineer from the Cisco Technical Assistance Center (TAC) can connect remotely to a customer's Catalyst Center setup for troubleshooting purposes.
Scheduler	Integrated with other back-end services, scheduler lets you run, schedule, and monitor network tasks and activities such as deploy policies, provision, or upgrade the network. You can also schedule rogue containment.
Search	Search for various objects in Catalyst Center, such as sites, network devices, clients, applications, policies, settings, tags, menu items, and more.

Display role-based access control statistics

You can display statistics that show how many users belong to each user role. You can also drill down to view the list of users who have a selected role.

Procedure

Step 1 From the main menu, choose **System** > **Users & Roles** > **Role Based Access Control**.

All default user roles and custom roles are displayed.

Step 2 Click the number corresponding to each user role to view the list of users who have that role.

Configure external authentication

If you are using an external server for authentication and authorization of external users, you should enable external authentication in Catalyst Center.

Before you begin

- Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure. For more information, see About user roles, on page 1.

- You must configure at least one authentication server.
- For SRBAC, you must define the access group on the Cisco ISE server.

  Configure the Cisco ISE server similar to how roles are configured in Catalyst Center. For example, <AAA attribute name>=rds=<comma separated list of rd names>. The first rd can be treated as the default access group profile.

Note When external authentication is enabled, Catalyst Center does not fall back to local users if the AAA server is unreachable or the AAA server rejects an unknown username.

When external authentication fallback is enabled, external users and local admins can log in to Catalyst Center.

To enable external authentication fallback, SSH to the Catalyst Center instance and enter this CLI command:

```
magctl rbac external_auth_fallback enable
```

Procedure

Step 1 From the main menu, choose **System** > **Users & Roles** > **External Authentication**.

Step 2 To enable external authentication in Catalyst Center, check the **Enable External User** check box.

Step 3 (Optional) Configure the AAA attribute.

For TACACS authentication, the following AAA attributes are supported:

Catalyst Center	TACACS
Empty	cisco-av-pair
cisco-av-pair	cisco-av-pair
Cisco-AVPair	Cisco-AVPair

For RADIUS authentication, the following AAA attributes are supported:

Catalyst Center	RADIUS
Empty	cisco-av-pair
Cisco-AVPair	cisco-av-pair

a) In the **AAA Attribute** field, enter the appropriate attribute for your use case, as described in the preceding tables. The default value of the **AAA Attribute** field is null.

b) Click **Update**.

Step 4 (Optional) Configure the AAA server or servers.

Configure these settings only if you want to swap the current primary or secondary AAA servers or define different AAA servers. From the main menu, choose **System** > **Settings** > **External Services** > **Authentication and Policy Servers** to open the **Authentication and Policy Servers** window.

a) From the **Primary AAA Server IP Address** drop-down list, choose the IP address of one of the preconfigured AAA servers.
b) From the **Secondary AAA Server IP Address** drop-down list, choose the IP address of one of the preconfigured AAA servers.
c) (Optional) If you are using a Cisco ISE server, you can update the settings, if necessary.

For information about Cisco ISE policies, see "Segmentation" in the *Cisco Identity Services Engine Administrator Guide*.

Table 2: Cisco ISE server settings

Name	Description
Shared Secret	Key for device authentications. The shared secret can contain up to 100 characters. The shared secret must be provided before the AAA address can be updated.
Username	Name that is used to log in to the Cisco ISE CLI.
Password	Password for the Cisco ISE CLI username.
FQDN	Fully qualified domain name (FQDN) of the Cisco ISE server. The FQDN consists of two parts, a hostname and the domain name, in the following format: *hostname.domainname.com* For example, the FQDN for a Cisco ISE server might be ise.cisco.com.
Subscriber Name	A unique text string—for example, `acme`—that is used during Catalyst Center-to-Cisco ISE integration to set up a new pxGrid client in Cisco ISE.
Virtual IP Address(es)	Virtual IP address of the load balancer behind which the Cisco ISE policy service nodes (PSNs) are located. If you have multiple PSN farms behind different load balancers, you can enter a maximum of six virtual IP addresses.

d) (Optional) To update advanced settings, click **View Advanced Settings** and update the settings, if necessary.

Table 3: AAA server advanced settings

Name	Description
Protocol	TACACS or RADIUS.
Authentication Port	Port used to relay authentication messages to the AAA server. • For RADIUS, the default is UDP port 1812. • For TACACS, the port is 49 and can’t be changed.
Accounting Port	Port used to relay important events to the AAA server. The information in these events is used for security and billing purposes. • For RADIUS, the default UDP port is 1813. • For TACACS, the port is 49 and can’t be changed.
Retries	Number of times that Catalyst Center can attempt to connect with Cisco ISE.

Name	Description
Timeout	Length of time that Catalyst Center waits for Cisco ISE to respond. The maximum timeout value is 60 seconds.

e) Click **Update**.

Two-factor authentication

Two-factor authentication, also known as 2FA, adds another layer of security to user verification by using an identifier method in addition to a user's name and password. The identifier method is generally something that only the actual intended user possesses (such as a phone app or keyfob) and is intentionally separated from the original login method.

The Catalyst Center implementation of two-factor authentication supports the use of a token client (that generates single-use token codes after the appropriate PIN is entered), a token server (that validates token codes), and an authentication server to manage user access. Authentication can be handled using either the RADIUS or TACACS+ protocol.

Prerequisites for two-factor authentication

The following prerequisites must be in place to set up two-factor authentication for use with Catalyst Center:

- An authentication server that is able to return attribute-value pairs to convey RBAC role authorizations for authenticated Catalyst Center users. In our example, we use Cisco Identity Services Engine (Cisco ISE) 2.3 Patch 1.
- A two-factor token server that you will integrate with your authentication server. In our example, we use RSA Authentication Manager 7.2.
- A token card application on the client’s machine that generates software tokens. In our example, we use RSA SecurID Software Token.

Two-factor authentication workflow

Here is a summary of what happens when a user logs in to a Catalyst Center appliance on which two-factor authentication has been configured:

1. In an RSA SecurID token client, a user enters their PIN to get a token code.
2. In the Catalyst Center login page, they enter their username and token code.
3. Catalyst Center sends the login request to Cisco ISE using either the RADIUS or TACACS+ protocol.
4. Cisco ISE sends the request to the RSA Authentication Manager server.
5. RSA Authentication Manager validates the token code and informs Cisco ISE whether the user has been authenticated successfully.
6. If the user has been authenticated, Cisco ISE matches the authenticated user with their configured authorization profile and returns the **role=NETWORK-ADMIN-ROLE** attribute-value pair.

7. Catalyst Center grants access to the features and pages associated with the user's role-based access control (RBAC) role.

Configure two-factor authentication

To configure two-factor authentication on your Catalyst Center appliance, complete the following procedure.

Procedure

Step 1 Integrate RSA Authentication Manager with Cisco ISE:

a) In RSA Authentication Manager, create two users: **`cdnac_admin`** (for the Admin user role) and **`cdnac_observer`** (for the Observer role).

For more information, see the "Add a User to the Internal Database" topic in the RSA Self-Service Console Help. To access this topic, do the following:

1. Open the *RSA Self-Service Console Help*.
2. In the **Search help** field, enter **`Add a User to the Internal Database`** and then click **Search help**.

b) Create a new authentication agent.

For more information, see the "Add an Authentication Agent" topic in the *RSA Self-Service Console Help*.

c) Generate the Authentication Manager agent configuration file (sdconf.rec):

1. From the RSA Security Console, choose **Access** > **Authentication Agents** > **Generate Configuration File**.

   The **Configure Agent Timeout and Retries** tab opens.
2. For the **Maximum Retries** and **Maximum Time Between Each Retry** fields, use the default values.
3. Click **Generate Configuration File**.

   The **Download Configuration File** tab opens.
4. Click the **Download Now** link.
5. When prompted, click **Save to Disk** to save a local copy of the zip file.
6. Unzip the file and use this version of the sdconf.rec file to overwrite the version that is currently installed on the agent.

d) Generate a PIN for the **`cdnac_admin`** and **`cdnac_observer`** users that you created in Step 1a.

For more information, see the "Create My On-Demand Authentication PIN" topic in the *RSA Self-Service Console Help*.

e) Start Cisco ISE, choose **Administration** > **Identity Management** > **External Identity Sources** > **RSA SecurID**, and then click **Add**.

f) In the **RSA SecurID Identity Sources** page, click **Browse**, choose the sdconf.rec file you downloaded, and then click **Open**.

g) Check the **Reauthenticate on Change PIN** check box, then click **Submit**.

Step 2 Create two authorization profiles, one for the Admin user role and one for the Observer user role.

a) In Cisco ISE, choose **Policy** > **Policy Elements** > **Results** > **Authorization** > **Authorization Profiles**.
b) For both profiles, enter the following information:

- **Name**: Enter the profile name.
- **Access Type**: Choose **ACCESS_ACCEPT**.
- **Advanced Attributes Settings** area: Choose **Cisco:cisco-av-pair** from the first drop-down list.

  If you are creating an authorization profile for the Admin user role, choose **Role=NETWORK-ADMIN-ROLE** from the second drop-down list.

  If you are creating an authorization profile for the Observer user role, choose **Role=OBSERVER-ROLE** from the second drop-down list.

Step 3 Create an authentication policy for your Catalyst Center appliance.

In the *Cisco Identity Services Engine Administrator Guide*, see the "Configure Authentication Policies" topic.

Step 4 Create two authorization policies, one for the Admin user role and one for the Observer user role.

In the *Cisco Identity Services Engine Administrator Guide*, see the "Configure Authorization Policies" topic.

Step 5 In the RSA Authentication Manager Security Console, verify that software tokens have been assigned to both users.

For more information, see the "View a Token" topic in the *RSA Self-Service Console Help*.

Note
If you need to assign tokens, complete the steps described in the "Assign a Software Token to a User" topic.

Enable two-factor authentication using RADIUS

To enable two-factor authentication that uses a Cisco ISE server configured for RADIUS, complete the following procedure:

Procedure

Step 1 Integrate Cisco ISE with Catalyst Center.

In the *Catalyst Center Installation Guide*, see the "Integrate Cisco ISE with Catalyst Center" topic.

Step 2 Configure Catalyst Center to use your Cisco ISE server for authentication.

See Configure External Authentication.

Important
Ensure that you specify the same shared secret for both Cisco ISE and Catalyst Center.

Enable two-factor authentication using TACACS+

To enable two-factor authentication that uses a Cisco ISE server configured for TACACS+, complete the following procedure:

Procedure

Step 1 In Cisco ISE, choose **Administration** > **Network Resources** > **Network Devices** to open the **Network Devices** window.

Step 2 Click **TACACS Authentication Settings** to view its contents. Ensure that a shared secret has already been configured for the Catalyst Center device that you added previously.

Step 3 Choose **Work Centers** > **Device Administration** > **Policy Elements** to open the **TACACS Profiles** window.

Step 4 Create TACACS+ profiles for the example_admin and example_observer user roles:

a) Click **Add**.

b) Complete the following tasks:

- Enter the profile name.
- After clicking the **Raw View** tab, enter the following text into the **Profile Attributes** text box:
  - For the example_admin user role, enter `Cisco-AVPair=ROLE=NETWORK-ADMIN-ROLE`
  - For the example_observer user role, enter `Cisco-AVPair=ROLE=OBSERVER-ROLE`

c) Click **Save**.

Step 5 Integrate Cisco ISE with Catalyst Center.

In the *Catalyst Center Installation Guide*, see the "Integrate Cisco ISE with Catalyst Center" topic.

Step 6 Configure Catalyst Center to use your Cisco ISE server for authentication.

See Configure External Authentication.

Important
Ensure that you specify the same shared secret for both Cisco ISE and Catalyst Center.

Log in using two-factor authentication

To log in to Catalyst Center using two-factor authentication, complete the following procedure:

Procedure

Step 1 From the Catalyst Center login page, enter the appropriate username.

Step 2 Open the RSA SecurID token client and enter the PIN you configured previously to generate a one-time token.

Step 3 Copy this token and paste it into the **Password** field of the Catalyst Center login page.

Step 4 Click **Log In**.

Display external users

You can view the list of external users who have logged in through RADIUS or TACACS for the first time. The information that is displayed includes their usernames and roles.

Procedure

Step 1 From the main menu, choose **System** > **Users & Roles** > **External Authentication**.

Step 2 Scroll to the bottom of the window, where the **External Users** area lists the external users.