Manage Users

About User Profiles

A user profile defines a user's login, password, and role (permissions).

You can configure both internal and external profiles for users. Internal user profiles reside in Cisco DNA 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 Cisco DNA 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 Cisco DNA 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 Cisco DNA 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 Cisco DNA Center functions. Users with an observer role cannot access any functions that configure or control Cisco DNA Center or the devices it manages.

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.

Step 1 Click the menu icon (≡) and 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. The password must contain:

- At least eight characters
- A character from at least three of the following categories:
  - Lowercase letter
  - Uppercase letter
  - Number
  - Special character

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.

Step 1 Click the menu icon (☰) and 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.

Step 1 Click the menu icon (☰) and 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**.

Reset a User Password

You can reset another user's password.

For security reasons, passwords are not displayed to any user, not even those 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.

Step 1 Click the menu icon (☰) and choose **System** > **Users & Roles** > **User Management**.

Step 2 Click the radio button next to the user whose password you want to reset.

Step 3 Click **Reset Password**.

Step 4 Enter a new password and confirm it. The new password must contain:

- At least eight characters
- A character from at least three of the following categories:

- Lowercase letter
- Uppercase letter
- Number
- Special character

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.

Step 1 Click the menu icon (≡) and 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.

Step 1 Click the menu icon, hover your cursor over **admin**, and choose **My Profile and Settings** > **My Account**.

Step 2 Click **Update Password**.

Step 3 Enter the current password, 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.

Step 1 Enter the following 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 the following:

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

Step 2 Enter the tenant-name in the following command to reset the password.

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

You are prompted to enter a new password.

Step 3 Enter a new password.

You are prompted to re-enter the new password to confirm.

Step 4 Enter the new password. The password is reset and you can log in to Cisco DNA Center using the new password.

Configure Role-Based Access Control

Cisco DNA 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 Cisco DNA 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.

Step 1 Define a custom role.

a) Click the menu icon (≡) and choose **System** > **Users & Roles** > **Role Based Access Control**.

b) Click **Create a New Role**.
The **Create a Role** window appears. If this is your first iteration of RBAC, after you have created the new role, you will be asked to assign users to the new role.

c) If a task overview window opens, click **Let’s do it** to go directly to the workflow.
The **Create a New Role** window appears.

d) Enter a name for the role and then click **Next**.
The **Define the Access** window appears with a list of options. By default, the observer role is set for all Cisco DNA Center functions.

e) 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.

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.

g) Click **Next**.
The **Summary** window appears.

h) In the **Summary** window, review the configuration settings. To make any changes, click **Edit**.
The **Done, *Role-Name*** window appears.

Step 2 To assign a user to the custom role you just created, click **Add Users**.

The **User Management** > **Internal Users** window appears, which allows you to assign the custom role to an existing user or to a new user.

- To assign the custom role to an existing user, do the following:

a. In the **Internal Users** window, click the radio button next to the user to whom you want to assign the custom role, and then click **Edit**.

   The **Update Internal User** slide-in pane appears.

b. From the **Role List** drop-down list, choose the custom role, and then click **Save**.

- To assign the custom role to a new user, do the following:

a. Click **Add**.

   The **Create Internal User** slide-in pane appears.

b. Enter the first name, last name, and username in the fields provided.

c. From the **Role List** drop-down list, choose the custom role to assign to the new user.

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 making changes to your access permissions, you must log out of Cisco DNA Center and then log back in for the new permission settings to take effect.

Cisco DNA Center User Role Permissions

Table 1: Cisco DNA Center User Role Permissions

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

Capability	Description
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 will affect Search and Assurance functionality.
Network Design	Set up 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, trustpool, cloud access keys, Stealthwatch, Umbrella, and data anonymization. • Export the device inventory and its credentials. **Note** To complete this task, you must have Read 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 Template Editor, Tagging, Model Config Editor, and Authentication Template. Note: To create SSIDs, you must have Write permission on **Network Settings**.
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**.
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.
Image Update	Upgrade software images on devices that don't match the Golden Image settings after a complete upgrade lifecycle.

Capability	Description
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 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 and Smart accounts.
Network Telemetry	Enable or disable the collection of application telemetry from devices. Configure the telemetry settings associated with the assigned site. Configure other settings like wireless service assurance and controller certificates. Note: To enable or disable network 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.
App 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.

Capability	Description
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**
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, and third-party app integrations.
APIs	Drive value by accessing Cisco DNA 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.

Capability	Description
System	Centralized administration of Cisco DNA 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 Cisco Credentials, Integrity Verification, Device EULA, HA, Integration Settings, Disaster Recovery, Debugging Logs, Telemetry Collection, System EULA, IPAM, vManage Servers, Cisco AI Analytics, Backup & Restore, and Data Platform.
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 Cisco DNA 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 Cisco DNA Center. With this role enabled, an engineer from the Cisco Technical Assistance Center (TAC) can connect remotely to a customer's Cisco DNA 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 Cisco DNA 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.

Step 1 Click the menu icon (≡) and 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 Cisco DNA 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.

Note In releases earlier than 2.1.x, when external authentication is enabled, Cisco DNA Center falls back to local users if the AAA server is unreachable or the AAA server rejects an unknown username. In the current release, Cisco DNA 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 Cisco DNA Center.

To enable external authentication fallback, SSH to the Cisco DNA Center instance and enter the following CLI command:

```
magctl rbac external_auth_fallback enable
```

Step 1 Click the menu icon (≡) and choose **System** > **Users & Roles** > **External Authentication**.

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

Step 3 (Optional) Configure the AAA attribute.

For TACACS authentication, the following AAA attributes are supported:

Cisco DNA 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:

Cisco DNA 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.

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. Click the menu icon (≡) and 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 "Configure and Manage Policies" 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 Cisco DNA 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 cannot be changed.

Name	Description
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 cannot be changed.
Retries	Number of times that Cisco DNA Center can attempt to connect with Cisco ISE.
Timeout	Length of time that Cisco DNA 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 Cisco DNA 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.

The topics in this section describe:

- The requirements that need to be in place in order to implement two-factor authentication.
- The necessary configuration settings you need to make.
- The Cisco DNA Center login procedure using two-factor authentication.

Prerequisites for Two-Factor Authentication

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

- An authentication server that is able to return attribute-value pairs to convey RBAC role authorizations for authenticated Cisco DNA 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 Cisco DNA 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 Cisco DNA Center login page, they enter their username and token code.
3. Cisco DNA 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 that the user has been authenticated successfully.
6. Cisco ISE matches the authenticated user with their configured authorization profile and returns the **role=NETWORK-ADMIN-ROLE** attribute-value pair.
7. Cisco DNA 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 Cisco DNA Center appliance, complete the following 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 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** field: Enter the profile's name.
- **Access Type** field: 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 Cisco DNA 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:

Step 1 Integrate Cisco ISE with Cisco DNA Center.

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

Step 2 Configure Cisco DNA 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 Cisco DNA 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:

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 and ensure that a shared secret has already been configured for the Cisco DNA Center device 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 cdnac_admin and cdnac_observer user roles:

a) Click **Add**.

b) Complete the following tasks:

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

c) Click **Save**.

Step 5 Integrate Cisco ISE with Cisco DNA Center.

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

Step 6 Configure Cisco DNA 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 Cisco DNA Center.

Log In Using Two-Factor Authentication

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

Step 1 From the Cisco DNA 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 in to the Cisco DNA Center login page's **Password** field.

Step 4 Click **Log In**.

Display External Users

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

Step 1 Click the menu icon (≡) and choose **System** > **Users & Roles** > **External Authentication**.

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