

Cisco Nexus Dashboard Admin Tasks, Release 3.2.x

Table of Contents

Roles and Permissions . . . 2
- Nexus Dashboard and Orchestrator Roles . . . 2
- Nexus Dashboard Insights . . . 3
- Nexus Dashboard Fabric Controller Roles . . . 3

Choosing Default Authentication Domain . . . 7

Remote Authentication . . . 8
- Configuring Remote Authentication Server . . . 8
- Adding LDAP as Remote Authentication Provider . . . 10
- Adding Radius or TACACS as Remote Authentication Provider . . . 12
- Editing Remote Authentication Domains . . . 13
- Deleting Remote Authentication Domains . . . 13

Multi-Factor Authentication . . . 14
- Configuring Okta Account as MFA Provider . . . 14
- Configuring MFA Client . . . 18
- Adding Okta as Remote Authentication Provider . . . 20
- Logging In To Nexus Dashboard Using MFA . . . 21

Users . . . 22
- Adding Local Users . . . 22
- Editing Local Users . . . 22

Security . . . 23
- Security Configuration . . . 23
- Security Domains . . . 24
- Validating Peer Certificates . . . 24
  - Exporting Certificate Chain From Cisco APIC . . . 25
  - Exporting Certificate Chain From Cisco NDFC . . . 26
  - Exporting Certificate Chain From Cisco DCNM . . . 26
  - Exporting Certificate Chain From Cisco Cloud Network Controller . . . 27
  - Importing Certificates Into Nexus Dashboard . . . 28

Trademarks . . . 29

You can choose how the users logging into the Nexus Dashboard GUI are authenticated. This release supports local authentication as well as LDAP, RADIUS, and TACACS remote authentication servers. User roles and permissions are described in this section, remote authentication configuration is described in Remote Authentication, and local user configuration is described in Users.

Roles and Permissions

Cisco Nexus Dashboard allows user access according to roles defined by role-based access control (RBAC). Roles are used in both local and external authentication and apply to either the Nexus Dashboard, the services running in it, or both. All roles can be assigned with read-only or write privileges. Read-only access allows the user to view objects and configurations, while write access allows them to make changes.

The following sections describes the user roles available in Nexus Dashboard and their associated permissions within the platform as well as the individual services.

The same roles can be configured on a remote authentication server and the server can be used to authenticate the Nexus Dashboard users. Additional details about remote authentication are available in the Remote Authentication section.

Nexus Dashboard and Orchestrator Roles

User Role	ND Platform	Orchestrator Service
Administrator	Provides full access to all settings, features, and tasks. The only role that allows adding and removing services.	Full access.
Approver	Same as Dashboard role.	Allows approval or denial of template configurations; does not allow editing or deploying templates.
Dashboard User	Allows access to the Dashboard view and launching applications; does not allow any changes to the Nexus Dashboard configurations.	No access.
Deployer	Same as Dashboard role.	Allows the user to deploy templates to fabrics; does not allow editing or approving templates.
Policy Manager	Same as Dashboard role.	No access.
Site Administrator	Allows access to configurations related to the fabric on-boarding and configuration.	Allows changing the fabric status between managed and unmanaged, as well as fabric resource template, fabric policy template, and monitoring template (access SPAN) configurations.

User Role	ND Platform	Orchestrator Service
Site Manager	Allows access to deployment of policies to the fabric.	Allows policy, schema, and monitoring template (tenant SPAN) configurations.
Tenant Manager	Same as Dashboard role.	Allows tenant policy, schema, and monitoring template (tenant SPAN) configurations.
User Manager	Allows access to users settings, such as creating users, changing permissions, and adding remote authentication providers.	No access.

Each role above is associated with a set of permissions, which in turn are used to show relevant and hide not relevant elements from the user's view.

Nexus Dashboard Insights

The Insights service does not support RBAC and any account that can log in to the Nexus Dashboard has full access to Insights.

Nexus Dashboard Fabric Controller Roles

User Role	Nexus Dashboard Fabric Controller
NDFC Access Admin	Allows you to perform operations related to network interfaces in NDFC's **Interface Manager** screen. An Access Admin user can perform the following actions: • Add, edit, delete and deploy layer 2 port channels, and vPC. • Edit host vPC, and ethernet interfaces. • Save, preview, and deploy from management interfaces. • Edit interfaces for LAN classic, and external fabrics if it isn't associated with policy. Except for nve, management, tunnel, subinterface, SVI, interface grouping, and loopback interfaces However, an Access Admin user cannot perform the following actions: • Cannot edit layer 3 port channels, ST FEX, AA FEX, loopback interfaces, nve interfaces, and subinterfaces • Cannot edit member interfaces and port channels of Layer 3, ST FEX, AA FEX • Cannot edit interfaces with policy associated from underlay and link • Cannot edit peer link port channel • Cannot edit management interface • Cannot edit tunnels
NDFC Change Approver	Users with this privilege can approve change control tickets. A user that is assigned with the NDFC Change Approver role can double-check changes that are associated with a specific ticket and approve or deny those changes.
NDFC Change Deployer	Users with this privilege can deploy change control tickets.
NDFC Device Upgrade Admin	Allows you to perform operations related to device upgrades in NDFC's **Image Management** screen.
NDFC Network Admin	Allows full administrative access.

User Role	Nexus Dashboard Fabric Controller
NDFC Network Operator	Allows read-only access the following NDFC menus: • Dashboard • Topology • Monitor • Applications A Network Operator user can view the following: • Fabric builder • Fabric settings • Preview configurations • Policies • Templates However, a Network Operator user cannot perform the following actions: • Cannot change expected configurations of any switch within any fabric • Cannot deploy any configurations to switches • Cannot access the administration options like licensing, creating more users, and so on

User Role	Nexus Dashboard Fabric Controller
NDFC Network Stager	Allows you to make configuration changes, but a Network Admin user will need to deploy the changes later. A Network Stager user can perform the following actions: • Edit interface configurations • View or edit policies • Create interfaces • Change fabric settings • Edit or create templates However, a Network Stager user cannot perform the following actions: • Cannot make any configuration deployments to switches • Cannot perform deployment-related actions from the DCNM Web UI or the REST APIs • Cannot access the administration options like licensing, creating more users, and so on • Cannot move switches in and out of maintenance mode • Cannot move fabrics in and out of deployment-freeze mode • Cannot install patches • Cannot upgrade switches • Cannot create or delete fabrics • Cannot import or delete switches  A Network Stager can only define intent for existing fabrics, but cannot deploy those configurations. A Network Admin can deploy the changes and edits that are staged by a user with the Network Stager role.

Choosing Default Authentication Domain

By default, the login screen will select the local domain for user authentication; you can manually change the domain at login time by selecting any of the available login domains from the dropdown menu.

Alternatively, you can set a different default login domain to the most commonly used as follows:



The domain must already exist before you can set it as the default domain. Adding remote authentication domains is described in Remote Authentication.

1. Navigate to your Nexus Dashboard's **Admin Console**.
2. Choose the default login domain.
   a. From the main navigation menu, select **Admin > Authentication**.
   b. In top right of the **Default Authentication** tile, click the **Edit** icon.

      The **Default Authentication** window opens.
3. In the **Default Authentication** that opens, choose the **Login Domain** from the dropdown.

Remote Authentication

Cisco Nexus Dashboard supports a number of remote authentication providers, including LDAP, TACACS, and Radius.

When configuring external authentication servers:

- You must configure each user on the remote authentication servers.
- All LDAP configurations are case sensitive.

  For example, if you have OU=Cisco Users on the LDAP server and OU=cisco users on the Nexus Dashboard, the authentication will not work.

- For LDAP configurations, we recommend using CiscoAVPair as the attribute string. If, for any reason, you are unable to use an Object ID 1.3.6.1.4.1.9.22.1, an additional Object IDs 1.3.6.1.4.1.9.2742.1-5 can also be used in the LDAP server.

  Alternatively, instead of configuring the Cisco AVPair values for each user, you can create LDAP group maps in the Nexus Dashboard.

- Single sign-on (SSO) between the Nexus Dashboard, fabrics, and applications is available for remote users only.
- When using SSO to cross-launch into an APIC fabric from your Nexus Dashboard's **Fabrics** page, the AV pairs defined for the Nexus Dashboard user are also used when logging into the APIC.

  For example, a user defined as admin for the Nexus Dashboard cluster will also have admin privileges in the APIC.

- When setting up remote authentication, AAA server must not be in the same subnet as the data interface.

Configuring Remote Authentication Server

When configuring the remote authentication server for the Nexus Dashboard users, you must add a custom attribute-value (AV) pair, specifying the username and the roles assigned to them.

The user roles and their permissions are the same as for the local users you would configure directly in the Nexus Dashboard GUI as described in Roles and Permissions.

The following tables list the Nexus Dashboard user roles and the AV pair you would use to define the roles on a remote authentication server, such as LDAP.

Nexus Dashboard AV Pairs

User Role	AV Pair Value
Administrator	admin
Approver	approver
Dashboard User	app-user
Deployer	deployer

User Role	AV Pair Value
Policy Manager	config-manager
Site Administrator	site-admin
Site Manager	site-policy
Tenant Manager	tenant-policy
User Manager	aaa



The app-user role is no longer valid and should be avoided.

Nexus Dashboard Fabric Controller AV Pairs

User Role	AV Pair Value
NDFC Access Admin	access-admin
NDFC Device Upgrade Admin	device-upg-admin
NDFC Network Admin	network-admin
NDFC Network Operator	network-operator
NDFC Network Stager	network-stager

The AV pair string format differs when configuring a read-write role, read-only role, or a combination of read-write and read-only roles for a specific user.

Note that ND must have its own AV pair value (such as "all//app-user|site-admin"), even if users are only using NDFC. The ND AV pair value of “app-user” is not sufficient for the NDFC administrator role. You must configure the AV pair value of "admin" or "site-admin" for the NDFC administrator. If you don’t configure the AV pair value, it can cause NDFC pages to not load properly.

A typical string includes the domain, followed by the read-write roles separated from the read-only roles using the slash (/) character; individual roles are separated by the pipe (|) character:

```
shell:domains=<domain>/<writeRole1>|<writeRole2>/<readRole1>|<readRole2>
```

For example, the following string illustrates how to assign the Tenant Manager and Policy Manager roles to a user, while still allowing them to see objects visible to the User Manager users:

```
shell:domains=all/tenant-policy|site-policy/aaa
```

Note that if you want to configure only the read-only or only read-write permissions for a user, you must still include the slash (/) character. The following examples show how to set just the read-write or read-only access to the objects available to Site Administrator role:

- Read-only: shell:domains=all//site-admin
- Read-write: shell:domains=all/site-admin/

Adding LDAP as Remote Authentication Provider



Beginning with Cisco Nexus Dashboard release 3.2.2m and later, the Message-Authenticator attribute is included in RADIUS Access-Accept, Access-Reject, and Access-Request packets sent to the RADIUS server. Due to this enforced behavior, the RADIUS server may require configuration changes to properly process the Message-Authenticator attribute. It is mandatory for the RADIUS server to enforce receiving this attribute. For additional security context, see Blast-RADIUS (CVE-2024-3596) Protocol Spoofing Mitigation.

Before you begin

- You must have at least one user already configured on the LDAP server as described in Configuring Remote Authentication Server.

  You will need to use an existing user for end-to-end verification of LDAP configuration settings.

To add an LDAP remote authentication provider:

1. Navigate to your Nexus Dashboard's **Admin Console**.
2. Add an authentication domain.
   a. From the main navigation menu, select **Admin > Authentication**.
   b. In the main pane, click the **Actions** menu and select **Create Login Domain**.
3. In the **Create Login Domain** screen that opens, provide domain details.
   a. Provide the **Name** for the domain.
   b. (Optional) Provide its **Description**.
   c. From the **Realm** dropdown, select Ldap.
   d. Then click **+Add Provider** to add a remote authentication server.

      The **Add Provider** window opens.
4. Provide the remote authentication server details.
   a. Provide the **Hostname** or **IP Address** of the server.
   b. (Optional) Provide the **Description** of the server.
   c. Provide the **Port** number.

      The default port is 389 for LDAP.

   d. Provide the **Base DN** and **Bind DN**.

      The Base DN and Bind DN depend on how your LDAP server is configured. You can get the Base DN and Bind DN values from the distinguished name of the user created on the LDAP server.

      Base DN is the point from which the server will search for users. For example, DC=nd,DC=local.

      Bind DN is the credentials used to authenticate against the server. For example, CN=admin,

CN=Users,DC=nd,DC=local.

e. Provide and confirm the **Key**.

This is the password for your Bind DN user. Anonymous bind is not supported, so you must provide a valid value in these fields.

f. Specify the **Timeout** and number of **Retries** for connecting to the authentication server.

g. Provide the **LDAP Attribute** field for determining group membership and roles.

The following two options are supported:

- ciscoAVPair (default)—used for LDAP servers configured with Cisco AVPair attributes for user roles.
- memberOf—used for LDAP servers configured with LDAP group maps. Adding a group map is described in a following step.

h. (Optional) Enable **SSL** for LDAP communication.

If you enable SSL, you must also provide the **SSL Certificate** and the **SSL Certificate Validation** type:

- Permissive: Accept a certificate signed by any certificate authority (CA) and use it for encryption.
- Strict: Verify the entire certificate chain before using it.

i. Choose **Default** or **Custom** in the **Filter Type** field.

If you choose **Custom** LDAP filter, a sample of a working syntax is (cn={username}).

j. (Optional) Enable **Server Monitoring**.

If you choose to enable monitoring, you must also provide the **Username** and **Password** for it.

k. In the **Validation** fields, provide a **Username** and **Password** of a user already configured on the LDAP server you are adding.

Nexus Dashboard will use this user to verify the end-to-end authentication to ensure that the settings you provided are valid.

l. Click **Save** to complete provider configuration.

m. Repeat this step for any additional LDAP authentication servers you want to use with this domain.

5. (Optional) Enable and configure **LDAP Group Map Rules**.

If you want to authenticate your LDAP users using Cisco AV pair strings, skip this step.

a. In the **LDAP Auth Choice**, select LDAP Group Map Rules.

b. Click **Add LDAP Group Map Rule**.

The **Add LDAP Group Map Rule** window opens.

c. Provide the **Group DN** for the group.

   The format depends on your LDAP tree. For example: DN=xxx,OU=xxx,DC=xxx and so on.

d. Select one or more **Roles** for the group.

e. Click **Save** to save the group configuration.

f. Repeat this step for any additional LDAP groups.

6. Click **Create** to finish adding the domain.

Adding Radius or TACACS as Remote Authentication Provider

Before you begin

- You must have at least one user already configured on the remote authentication server as described in Configuring Remote Authentication Server.

  You will need to use an existing user for end-to-end verification of the provider configuration settings.

To add a Radius or TACACS remote authentication provider:

1. Navigate to your Nexus Dashboard's **Admin Console**.
2. Add an authentication domain.
   a. From the main navigation menu, select **Admin > Authentication**.
   b. In the main pane, click the **Actions** menu and select **Create Login Domain**.
3. In the **Create Login Domain** screen that opens, provide domain details.
   a. Provide the **Name** for the domain.
   b. (Optional) Provide its **Description**.
   c. From the **Realm** dropdown, select Radius or Tacacs.
   d. Then click **+Add Provider** to add a remote authentication server.

      The **Add Provider** window opens.
4. Provide the remote authentication server details.
   a. Provide the **Hostame** or **IP Address** of the server.
   b. (Optional) Provide the **Description** of the server.
   c. Choose **Authorization Protocol** used by the server.

      You can choose PAP, CHAP, or MS-CHAP.

   d. Provide the **Port** number.

      The default port is 1812 for RADIUS and 49 for TACACS

   e. Provide and confirm the **Key**.

This is the password used for connecting to the provider server.

f. (Optional) Choose whether you want to enable **Server Monitoring**.

If you choose to enable monitoring, you must also provide the **Username** and **Password** for it.

g. In the **Validation** fields, provide a **Username** and **Password** of a user already configured on the remote server you are adding.

Nexus Dashboard will use this user to verify the end-to-end authentication to ensure that the settings you provided are valid.

h. Click **Save** to complete provider configuration.

i. Repeat this step for any additional remote authentication servers.

5. Click **Create** to finish adding the domain.

Editing Remote Authentication Domains

If you want to make changes to a domain you have created:

1. Navigate to your Nexus Dashboard's **Admin Console**.
2. From the main navigation menu, select **Admin > Authentication**.
3. From the **Actions** menu for the domain, select **Edit Login Domain**.

You cannot change the name and the type of the authentication domain, but you can make changes to the description and provider configuration.



If you make any changes to the login domain, including simply updating the description, you must re-enter the key for all existing providers.

Deleting Remote Authentication Domains

1. Navigate to your Nexus Dashboard's **Admin Console**.
2. From the main navigation menu, select **Admin > Authentication**.
3. From the **Actions** menu for the domain, select **Delete Login Domain**.
4. In the **Confirm Delete** prompt, click **OK** to confirm.

Multi-Factor Authentication

Starting with Release 2.1.2, you can configure your Nexus Dashboard to use multi-factor authentication (MFA) for user login.

When configuring multi-factor authentication:

- You will configure each user in your MFA provider, as described in Configuring Okta Account as MFA Provider

  This release supports only Okta as MFA provider.

- You will establish MFA provider and client integration, as described in Configuring MFA Client.

  This release supports only Duo as MFA client.

- You will add the MFA provider as an external authentication domain in Nexus Dashboard, as described in Adding Okta as Remote Authentication Provider.

Configuring Okta Account as MFA Provider

The following steps provide basic configuration required to enable MFA for Nexus Dashboard using Okta as a provider. Detailed Okta configurations are outside the scope of this document, see Okta documentation for all available options.

To configure Okta for Nexus Dashboard MFA:

1. Log in to your Okta account.

   To create an account, browse to https://developer.okta.com.

2. Create a new app integration.
   a. From the left navigation menu, select **Applications > Applications**.
   b. Click **Create App Integration**.
   c. For **Sign-in method**, select OIDC - OpenID Connect.
   d. For **Application Type**, select Web Application.
   e. Click **Next**.
   f. Provide **App integration name**, for example, nd-mfa.

      The following steps assume you used nd-mfa as the app integration name. If you choose a different name, replace nd-mfa where appropriate.

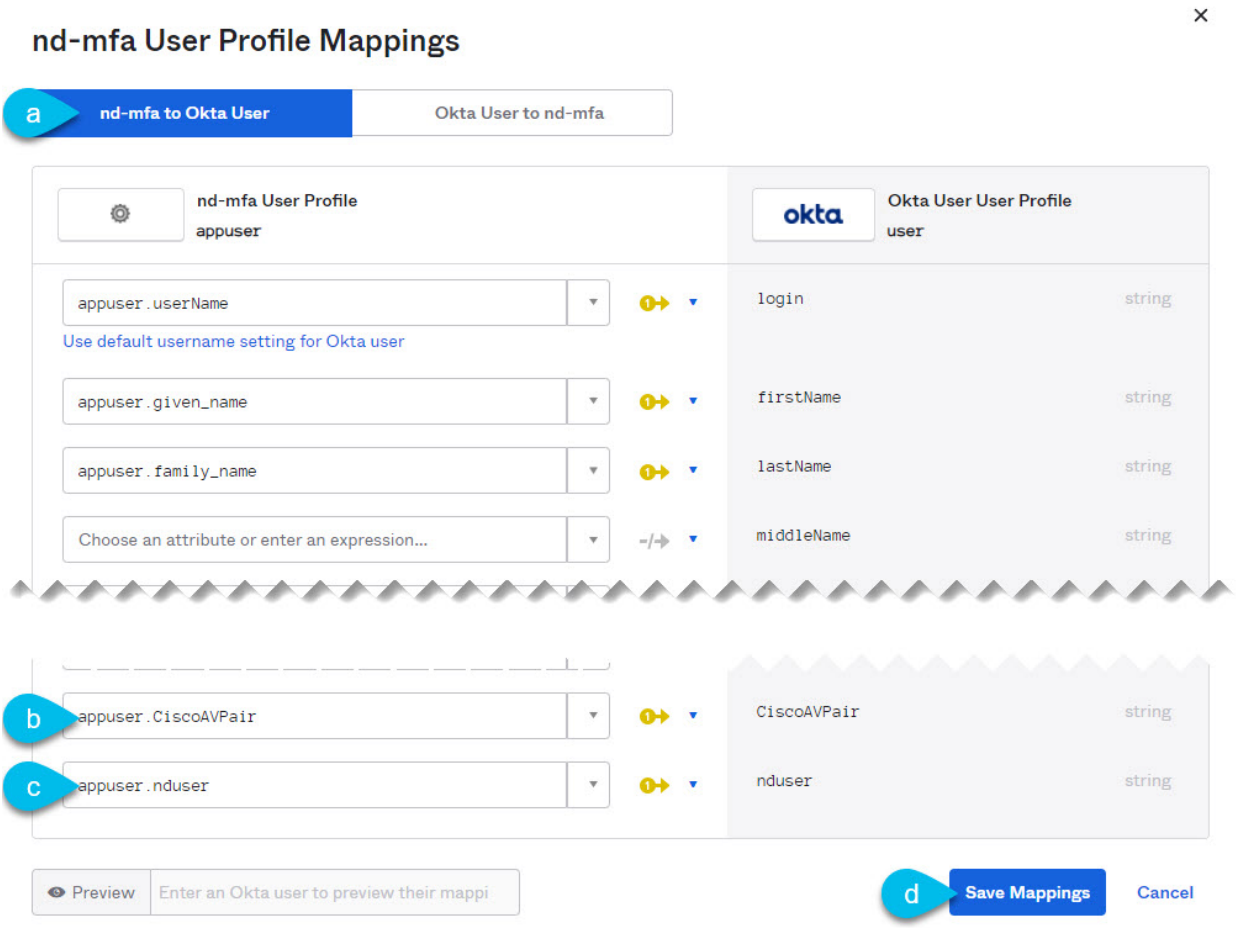
   g. For **Sign-in redirect URIs**, enter https://<nd-node1-ip>/oidccallback

      Replace the <nd-node1-ip> with your cluster node IP address, then click **+Add URI** to provide the URIs for all nodes in the cluster.

   h. For **Controlled Access**, choose Skip group assignment for now.
   i. Leave other fields at their default values and click **Save**.

3. Add the required attributes to the default user.
    a. From the left navigation menu, select **Directory > Profile Editor**.
    b. Click the **Okta User (default)** profile.
    c. Click **+Add Attribute**.
    d. For **Data type**, choose string.
    e. For **Display name**, **Variable name**, and **Description**, enter CiscoAVPair.
    f. Ensure that **Attribute required** is unchecked.
    g. Leave other fields at default values and click **Save and Add Another**.
    h. For **Data type**, choose string.
    i. For **Display name**, **Variable name**, and **Description**, enter nduser.
    j. Ensure that **Attribute required** is unchecked.
    k. Leave other fields at default values and click **Save**.
4. Add the required attributes to the nd-mfa user you created.
    a. From the left navigation menu, select **Directory > Profile Editor**.
    b. Click the **nd-mfa User (default)** profile.
    c. Click **+Add Attribute**.
    d. For **Data type**, choose string.
    e. For **Display name**, **Variable name**, and **Description**, enter CiscoAVPair.
    f. Ensure that **Attribute required** is checked.
    g. Leave other fields at default values and click **Save and Add Another**.
    h. For **Data type**, choose string.
    i. For **Display name**, **Variable name**, and **Description**, enter nduser.
    j. Ensure that **Attribute required** is checked.
    k. Leave other fields at default values and click **Save**.
5. Map the attributes.
    a. From the left navigation menu, select **Directory > Profile Editor**.
    b. Click the **nd-mfa User** profile.
    c. In the **Attributes** area of the main window, click **Mappings**.

        The **nd-mfa User Profile Mappings** window opens.



d. At the top of the **nd-mfa User Profile Mappings** window, click **nd-mfa to Okta User**.

e. Select app.CiscoAVPair from the dropdown menu next to CiscoAVPair.

f. Select app.nduser from the dropdown menu next to nduser.

g. Click **Save Mappings**.

h. Click **Apply updates now**.

6. Create users.

   a. From the left navigation menu, select **Directory > People**.

   b. Click **+Add person**.

   c. Provide the user information.

   d. Click **Save and Add Another** to add another user or click **Save** to finish.

      You must add all users that you want to be able to log in to your Nexus Dashboard.

7. Assign users to the app.

   a. From the left navigation menu, select **Applications > Application**.

   b. Click the application you created (nd-mfa).

   c. Select the **Assignments** tab.

   d. Choose **Assign > Assign to People**.

      The **Assign nd-mfa to People** window opens.

e. In the **Assign nd-mfa to People** window, click **Assign** next to the user you want to be able to log in to your Nexus Dashboard.

f. In the user details window that opens, provide a value for **CiscoAVPair** and **nduser** fields.

The **CiscoAVPair** values are described in the Configuring Remote Authentication Server, for example shell:domains=all/admin/.

The **nduser** value will be used as the username for this user when logging in to your Nexus Dashboard.

g. Click **Save and Go Back**.

h. Assign another user or click **Done** to finish.

You must add all users that you created in a previous step.

8. Configure **Claims** for the app.

a. From the left navigation menu, select **Security > API**.

b. Click the **default** name.

c. Select the **Claims** tab.

d. Click **+Add Claim** to add the CiscoAVPair claim.

e. In the **Name** field, enter CiscoAVPair.

f. From the **Include in token type** dropdown, select ID Token.

We recommend using ID Token, however Access Token is also supported.

g. In the **Value** field, enter appuser.CiscoAVPair.

h. Click **Save**.

i. Click **+Add Claim** to add the nduser claim.

j. In the **Name** field, enter nduser.

k. From the **Include in token type** dropdown, select ID Token.

You must create both claims in the same token, mixing ID Token and Access Token is not supported.

l. In the **Value** field, enter appuser.nduser.

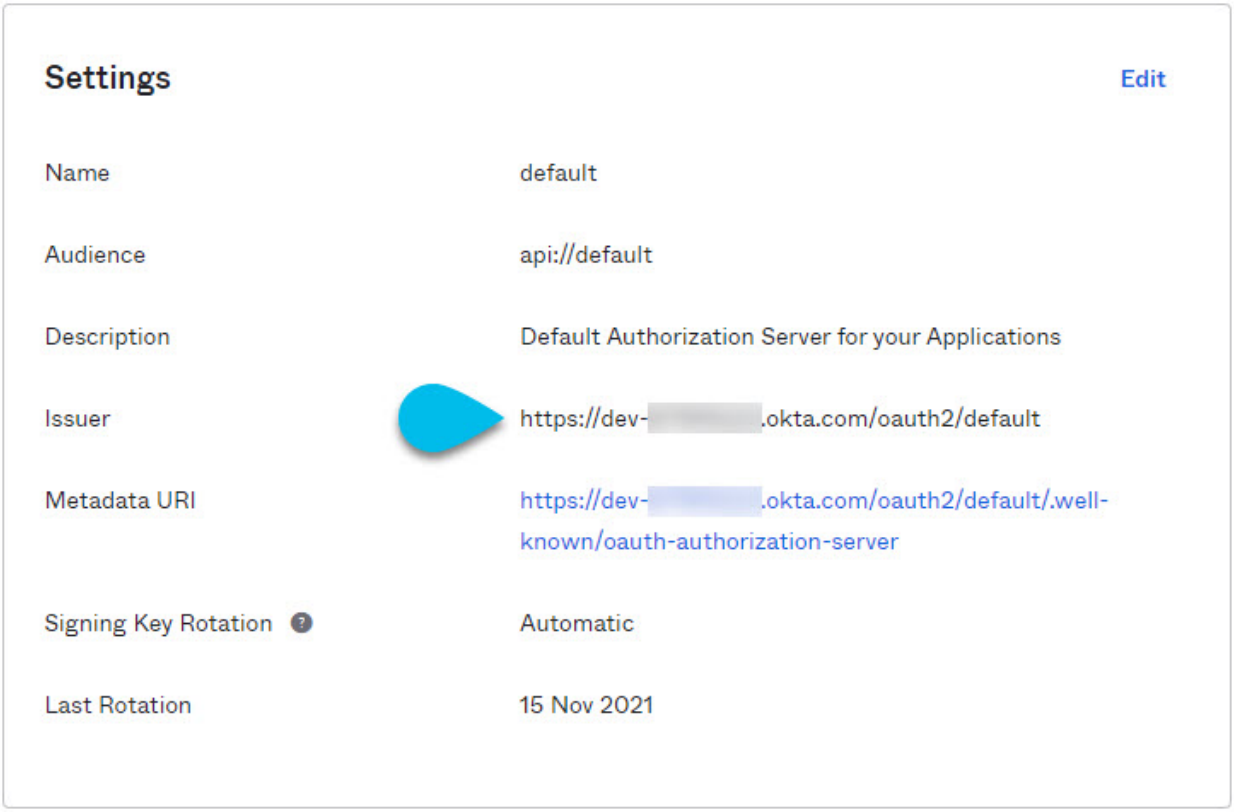
m. Click **Save**.

9. Gather the required Okta account information for adding it as authentication provider for your Nexus Dashboard.

a. From the left navigation menu, select **Security > API**.

b. Click the **default** name.

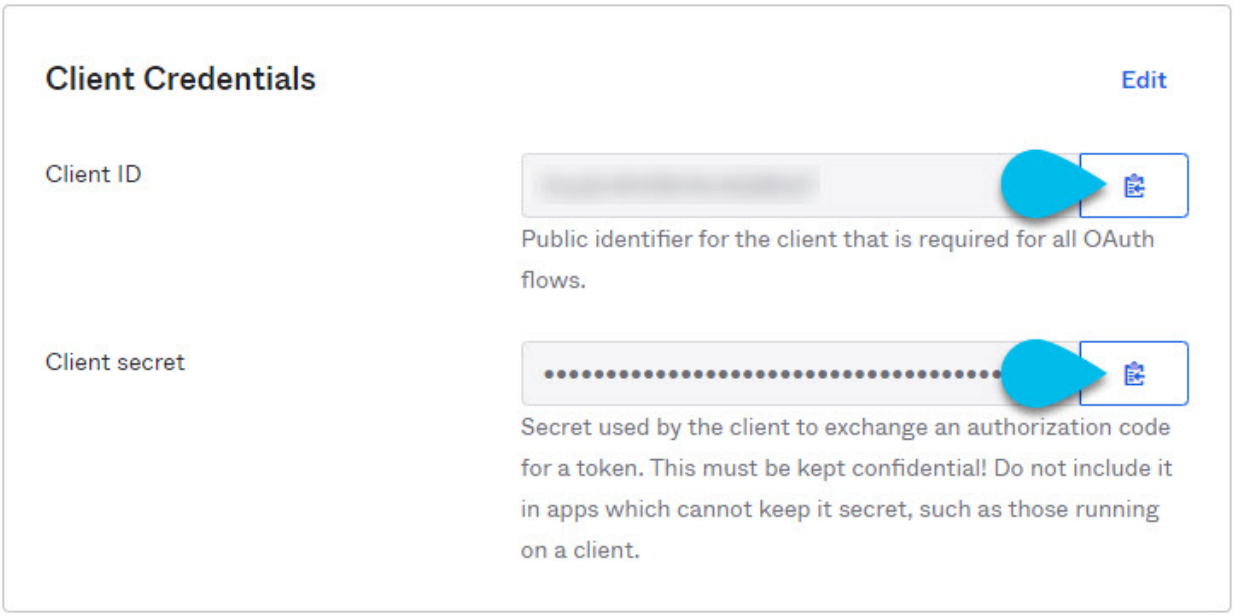
c. Note down the **Issuer** value.



d. From the left navigation menu, select **Application > Applications**.

e. Click the application you created (nd-mfa).

f. Note down the **Client ID** and **Client Secret** values.



Configuring MFA Client

This release supports only Cisco Duo as MFA client.

The following steps provide basic configuration required to enable using Cisco Duo for Nexus Dashboard MFA. Detailed Duo configurations are outside the scope of this document, see Cisco Duo documentation for all available options.

To configure Duo:

1. Log in to your Okta account.
2. Add DUO as an MFA type.
   a. From the left navigation menu, select **Security > Multifactor**.
   b. In the **Factor Types** tab, select Duo Security.

      If you do not have the Duo Security option, you will need to open a support case with Okta from https://support.okta.com/help/s/opencase.

   c. In the **Duo Security** window, provide the required information.

      For more information on how to obtain integration key, secret key, and API hostname, see https://duo.com/docs/okta.

      Ensure that **Duo Username Format** is set to Email.

   d. Click **Save**.
3. Create a Duo rule.
   a. From the left navigation menu, select **Applications > Application**.
   b. Click the application you created (nd-mfa).
   c. Select the **Sign On** tab.
   d. In the **Sign On Policy** area, click **+Add Rule**.
   e. Provide the name for the rule.
   f. In the **Access** area, enable **Prompt for factor** and select **Every sign on**.
   g. Specify other options as required by your use case.
   h. Click **Save**.
4. Configure Okta and Duo integration.

   There are two ways you can allow the users you configured in Okta to use the Duo app for MFA—have the Duo admin add all the same users in Duo dashboard or have each individual user log in to Okta and self-enroll.

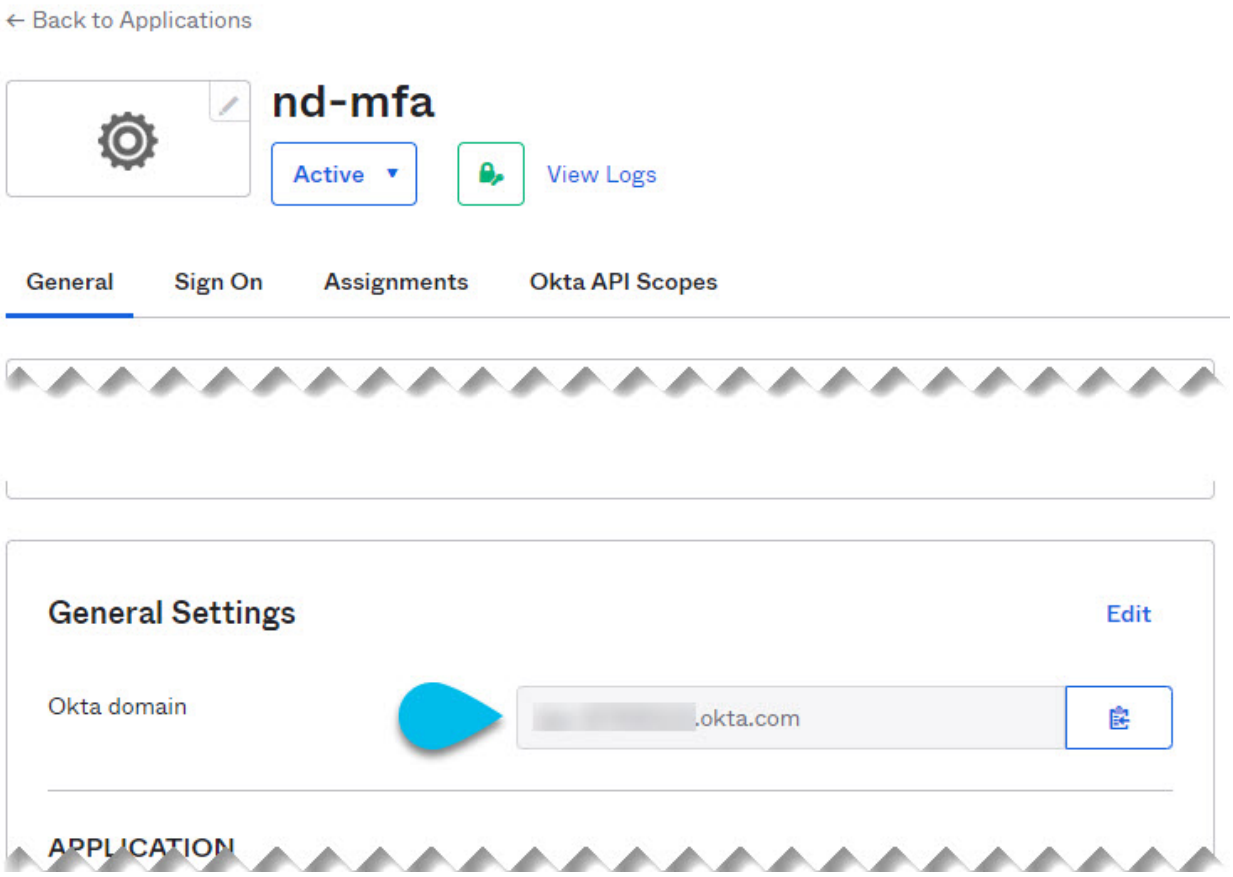
   To configure users in Duo dashboard:

   a. Log in to your Duo dashboard as admin user.
   b. From the left navigation menu, select **Users**.
   c. Click **Add User** and provide the details that match the user's information in Okta.
   d. Repeat this step for all users you added in Okta.

   To self-enroll:

   a. Instruct every user you created in Configuring Okta Account as MFA Provider to log in to Okta on their own using your specific Okta domain.

      You can determine the Okta domain to use by navigating to **Application > Application**, then clicking the nd-mfa application you created and copying the **Okta domain** URL:



b. Once they're logged in, they can navigate to the **Settings** page from the top right user menu.

c. Choose **Duo Security Setup** and follow the instructions on the screen.

Adding Okta as Remote Authentication Provider

Before you begin

- You must have at least one user already configured in Okta as described in Configuring Okta Account as MFA Provider.
- You must have the **Client ID**, **Client Secret**, and **Issuer** information from your Okta account available, which is described in the last step of Configuring Okta Account as MFA Provider.
- If you want to use a proxy to connect to your Okta account, the proxy must already be configured as described in System Settings.

To add Okta as remote authentication provider:

1. Log in to your Nexus Dashboard as an admin user.
2. Navigate to the **Admin Console**.
3. Add an authentication domain.
   a. From the main navigation menu, select **Admin > Authentication**.
   b. In the main pane, click the **Actions** menu and select **Create Login Domain**.
4. In the **Create Login Domain** screen that opens, provide domain details.
   a. Provide the **Name** for the domain.
   b. (Optional) Provide its **Description**.

c. From the **Realm** dropdown, select OIDC.

d. In the **Client ID** field, enter the client ID you obtained from your Okta account.

e. In the **Client Secret** field, enter the client secret you obtained from your Okta account.

f. In the **Issuer** field, enter the URI you obtained from your Okta account.

g. (Optional) Check the **User Proxy** option if you want to connect to Okta over a proxy.

h. Leave the **Scopes** options unchecked.

This release supports the openid scope only.

5. Click **Create** to finish adding the domain.

Logging In To Nexus Dashboard Using MFA

1. Navigate to one of your Nexus Dashboard IPs as your typically would.
2. From the **Login Domain** dropdown, select the OIDC domain you created in Adding Okta as Remote Authentication Provider.

   The **Username** and **Password** fields will not be displayed.
3. Click **Login**.

   You will be redirected to the Okta login page.
4. Log in using a user that was configured in Okta as described in Configuring Okta Account as MFA Provider.

   A push notification will be sent to your Duo client.
5. Approve the login using Duo.

   You will be redirected back to the Nexus Dashboard UI and logged in using the Okta user.

Users

The **Users** GUI page allows you to view and manage all users that have access to the Nexus Dashboard.

The **Local** tab displays all local users while the **Remote** tab displays users that are configured on the remote authentication servers you have added as described in the Remote Authentication section.



- The default local admin user cannot be deleted.
- Single sign-on (SSO) between the Nexus Dashboard, fabrics, and applications is available for remote users only. For more information on configuring remote users, see Remote Authentication.

Adding Local Users

1. Navigate to your Nexus Dashboard's **Admin Console**.
2. Create a new local user.
    a. From the main navigation menu, select **Admin > Users**.
    b. In the main pane, click **Create Local User**.
3. In the **Create Local User** screen that opens, provide user details.
    a. Provide the **User ID** that will be used for loggin in.
    b. Provide and confirm the initial **Password**.
    c. Provide the **First Name**, **Last Name**, and **Email Address** for the user.
    d. Choose the user's **Roles** and **Privileges**.

        You can select one or more roles for each user. The available roles and their permissions are described in Roles and Permissions.

        For all of the user roles you select, you can choose to enable read-only or read-write access. In case of read-only access, the user will be able to view the objects and settings allowed by their user **Role** but unable to make any changes to them.

    e. Click **Create** to save the user.

Editing Local Users

1. Navigate to your Nexus Dashboard's **Admin Console**.
2. Open user details screen.
    a. From the main navigation menu, select **Admin > Users**.
    b. In the main pane, click on the user's name.
    c. In the details pane that opens, click the **Details** icon.
3. In the ***<user-name>*** details screen that opens, click the **Edit** icon.
4. In the **Edit User** screen that opens, update the settings as necessary.

Security

The **Security** GUI page allows you to view and manage certificates used by the Nexus Dashboard.

Security Configuration

The **Administrative > Security Configuration** page allows you to configure authentication session timeouts and security certificates used by your Nexus Dashboard cluster.

Before you begin

- You must have the keys and certificates you plan to use with Nexus Dashboard already generated.

  Typically, this includes the following files:

  - Private key (nd.key)
  - Certificate Authority's (CA) public certificate (ca.crt)
  - CA-signed certificate (nd.crt)

  Generating these files for self-signed certificates is described in Generating Private Key and Self-Signed Certificate.

- We recommend creating a configuration backup of your Nexus Dashboard cluster before making changes to the security configurations.

  For more information about backups, see " Backup and Restore" in Nexus Dashboard Operations.

To edit security configuration:

1. Navigate to your Nexus Dashboard's **Admin Console**.
2. Edit security configuration.
   a. From the main navigation menu, select **Admin > Security**.
   b. In the main pane, select the **Security Configuration** tab.
   c. In the main pane, click the **Edit** icon.
3. In the **Security Configuration** screen that opens, update one or more fields as required:

   Note that uploading the keys and certificate files is not supported and you will need to paste the information in the following fields.

   a. Update the **Session Timeout**.

      This field defines the duration of the API tokens with the default duration set to 20 minutes.

   b. Update the **Idle Timeout**.

      This field defines the duration of the UI session.

   c. In the **Domain Name** field, provide your domain.
   d. Select **Check the Enforce Strict Content Security Policy** to disable Qualtrics integration from the browser at a system wide level.

e. Click the **SSL Ciphers** field and select any additional cipher suites you want to enable from the dropdown or click the **x** icon on an existing cipher suite to remove it.

   Cipher suites define agorithms (such as key exchange, bulk encryption, and message authentication code) used to secure a network connection. This field allows you to customize which cipher suites your Nexus Dashboard cluster will use for network communication and disable any undesired suites, such as the less secure TLS1.2 and TLS1.3.

f. In the **Key** field, provide your private key.

g. In the **RSA Certificate** field, provide the CA-signed or self-signed certificate.

h. In the **Root Certificate** field, provide the CA's public certificate.

i. (Optional) If your CA provided an Intermediate Certificate, provide it in the **Intermediate Certificate** field.

j. Click **Save** to save the changes.

   After you save your changes, the GUI will reload using the new settings.

Security Domains

A restricted security domain allows an administrator to prevent a group of users from viewing or modifying any objects created by a group of users in a different security domain, even when users in both groups have the same assigned privileges.

For example, an administrator in restricted security domain (domain1) will not be able to see fabrics, services, cluster or user configurations in another security domain (domain2).

Note that a user will always have read-only visibility to system-created configurations for which the user has proper privileges. A user in a restricted security domain can be given a broad level of privileges within that domain without the concern that the user could inadvertently affect another group's physical environment.

To create a security domain:

1. Navigate to your Nexus Dashboard's **Admin Console**.
2. Create a new security domain.
   a. From the main navigation menu, select **Admin > Security**.
   b. In the main pane, select the **Security Domains** tab.
   c. In the main pane, click **Create Security Domain**.
3. In the **Create Security Domain** screen that opens, provide the domain details.
   a. Provide the **Name** for the domain.
   b. (Optional) Provide a description for the domain.
   c. Click **Create** to save the domain.

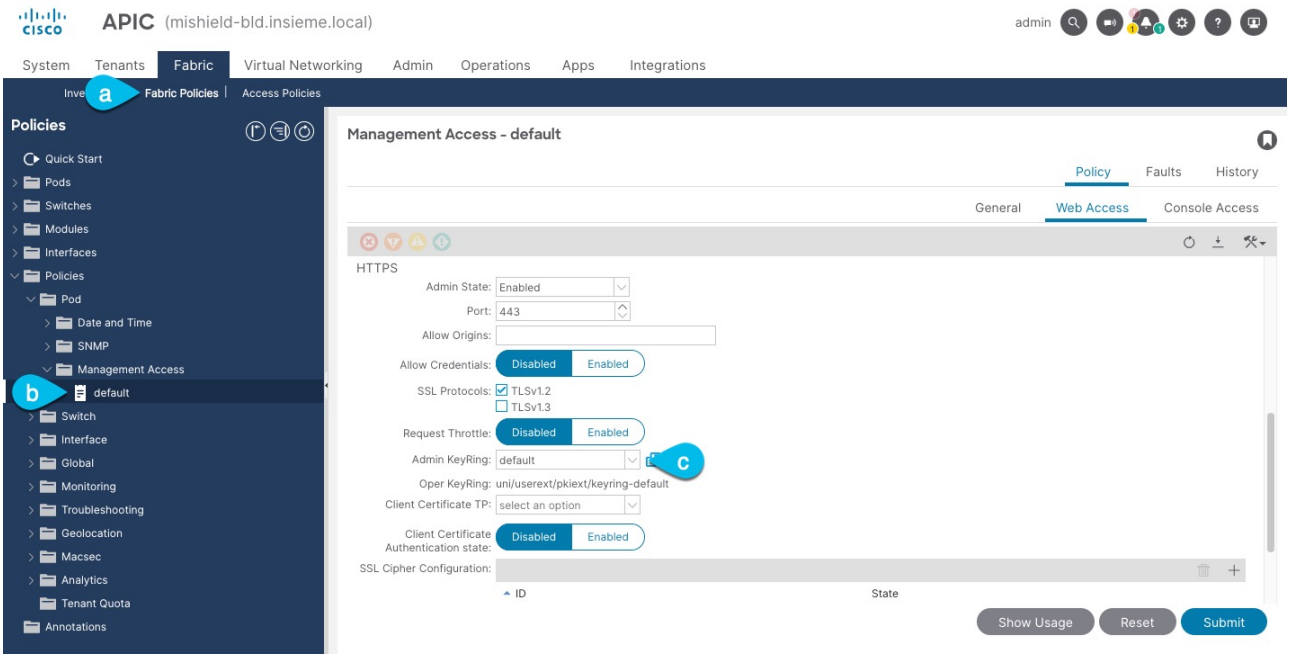
Validating Peer Certificates

You can import a fabric controller's Certificate Authority (CA) root certificate chain into Nexus Dashboard. This allows you to verify that the certificates of hosts to which your Nexus Dashboard

connects (such as fabric controllers) are valid and are signed by a trusted Certificate Authority (CA) when you add the fabrics.

Exporting Certificate Chain From Cisco APIC

1. Log in to your Cisco APIC.
2. Check which key ring is being used for management access:



   a. In the top navigation bar, choose **Fabric > Fabric Policies**.

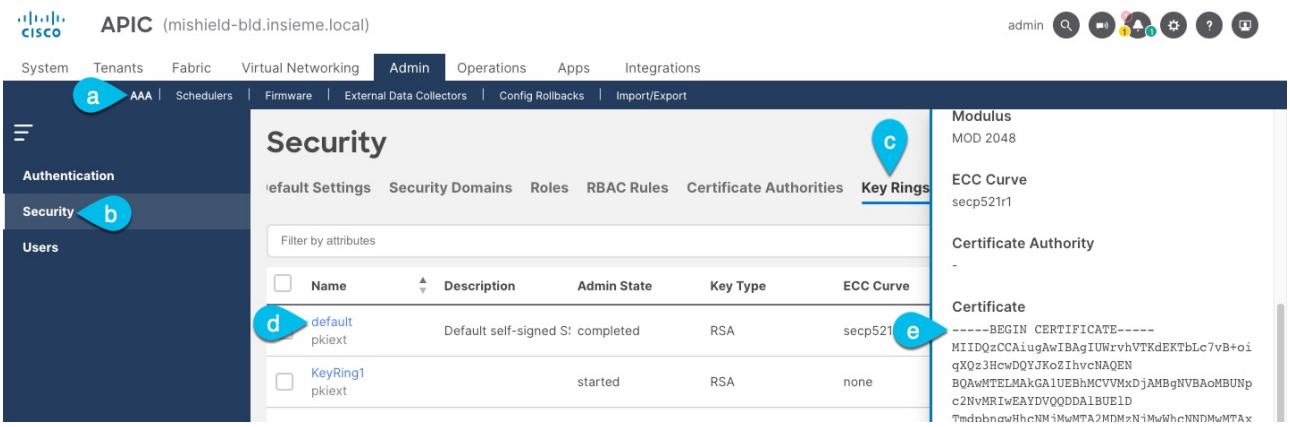
   b. In the left navigation menu, choose **Policies > Pod> Management Access**.

   c. In the main pane, note the name in the **Admin KeyRing** field.

      In the above example, the default key ring is being used. However, if you created a custom key ring with a custom certificate chain, the name of that key ring would be listed in the **Admin KeyRing** field.

      Custom security configuration for Cisco APIC is described in detail in *Cisco APIC Security Configuration Guide* for your release.

3. Export the certificate used by the key ring:



a. In the top navigation bar, choose **Admin > AAA**.
b. In the left navigation menu, choose **Security**.
c. In the main pane, choose the **Key Rings** tab.
d. Click the name of the key ring you found in the previous step and copy the **Certificate**.

The above example shows the default key ring from the previous step. However, if you had a custom key ring configured, choose the CA certificate chain used to create the key ring.

You must include the -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- in the text you copy, for example:

```
-----BEGIN CERTIFICATE-----
MIIDQzCCAiugAwIBAgIUWrvhVTKdEKTbLc7vB+oiqXQz3HcwDQYJKoZIhvcNAQEN
[...]
-----END CERTIFICATE-----
```

Exporting Certificate Chain From Cisco NDFC

1. Log in to the Nexus Dashboard that's hosting the service.

   In case of NDFC, there is no separate certificate from the service so you use the Nexus Dashboard host's certificate.

2. Export the certificate.
   a. In the main navigation menu, choose **Admin > Security**.
   b. In the main pane, choose the **Security Configuration** tab
   c. In the **Security Configuration** page, click the **Edit** icon.
   d. Copy the **Root Certificate**.



We recommend copying the certificate chain from the **Edit** page instead of directly from the **Security Configuration** page to ensure that there are no spaces or new line characters (\n) in the string you copy.

You must include the -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- in the text you copy, for example:

```
-----BEGIN CERTIFICATE-----
MIIDhTCCAm2gAwIBAgIIOqlnNF7g9e8wDQYJKoZIhvcNAQELBQAwSzELMAkGA1UE
[...]
-----END CERTIFICATE-----
```

Exporting Certificate Chain From Cisco DCNM

1. SSH in to you Cisco DCNM as the sysadmin user.

Unlike the other fabric controllers, DCNM certificates are not available in the UI, so you must use the CLI.

```
# ssh -l sysadmin <dcnm-ip-address>
```

2. Change into the /var/lib/dcnm/afw/apigateway/ directory.

   The certificate (dcnmweb.crt) file is located in this directory.

```
dcnm# cd /var/lib/dcnm/afw/apigateway/
dcnm# ls -ltr /* View the contents of the folder
total 128
-rw------- 1 root root 1844 Nov 18 13:14 dcnmweb.key.2019-11-20T132939-08:00
-rw-r--r-- 1 root root 1532 Nov 18 13:14 dcnmweb.crt.2019-11-20T132939-08:00
-rw------- 1 root root 1844 Nov 20 10:15 dcnmweb.key.2019-11-20T132950-08:00
-rw-r--r-- 1 root root 1532 Nov 20 10:15 dcnmweb.crt.2019-11-20T132950-08:00
-rw------- 1 root root 1844 Dec 22 13:59 dcnmweb.key
-rw-r--r-- 1 root root 1532 Dec 22 13:59 dcnmweb.crt
```

3. Check for root certificate.

   Depending on which Certificate Authority you used to sign your certificate, the root certificate may be included in the dcnmweb.crt file or may be provided as a separate file.

   To check whether the root certificate is included:

   dcnm# openssl x509 -text -noout -in *dcnmweb.crt*

   If the file includes the root certificate, copy it. Otherwise, use the root certificate file you should have obtained when signing your certificate.

Exporting Certificate Chain From Cisco Cloud Network Controller

1. Log in to your Cisco Cloud Network Controller.
2. Export the certificate.
   a. In the main navigation menu, choose **Admin > Security**.
   b. In the main pane, choose the **Key Rings** tab.
   c. Click the name of the certificate you want to import into your Nexus Dashboard and copy the **Certificate Authorities**.

      The above example shows the default key ring. However, if you had a custom key ring configured, choose the CA certificate chain used to create the key ring.

      You must include the -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- in the text you copy, for example:

```
-----BEGIN CERTIFICATE-----
MIIDvTCCAqWgAwIBAgIJAI6W9R8DXDgLMA0GCSqGSIb3DQEBDQUAMEAxCzAJBg
NV
[...]
-----END CERTIFICATE-----
```

Importing Certificates Into Nexus Dashboard

1. Log in to your Nexus Dashboard where you plan to onboard the fabrics.
2. Import the certificate into Nexus Dashboard.
    a. Log in to your Nexus Dashboard where you will onboard the fabrics.
    b. In the left navigation menu, choose **Admin > Security**.
    c. In the main pane, select the **CA Certificates** tab.
    d. Click **Add CA certificate**, provide a unique name for the certificate, and paste the certificate chain you copied from your fabric's controller.
3. Proceed with adding the fabric as you typically would, but enable the **Verify Peer Certificate** option.

    Note that if you enable the **Verify Peer Certificate** option but don't import the valid certificate, fabric onboarding will fail.

    Adding fabrics is described in Adding Fabrics.

Trademarks

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2017-2025 Cisco Systems, Inc. All rights reserved.

First Published: 2024-03-01
Last Modified: 2024-03-01

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883