

Configuring Users, Roles, and Security, Release 4.3.1

Table of Contents

New and changed information . . . 1
Roles and permissions . . . 2
Understanding roles and permissions before and after the unified product . . . 2
Roles and permissions in the unified releases . . . 2
Mapping roles from non-unified releases . . . 3
Mapping Nexus Dashboard and Orchestrator roles . . . 4
Mapping Nexus Dashboard Fabric Controller roles . . . 4
Choosing a default authentication domain . . . 5
Multi-factor authentication . . . 6
Add Okta as a remote authentication provider . . . 6
Logging in to Nexus Dashboard using MFA . . . 7
Configure an Okta account as an MFA provider . . . 7
Configure an MFA client . . . 11
Microsoft Entra ID multi-factor authentication (MFA) . . . 14
Guidelines and limitations . . . 14
Add Microsoft Entra ID as a remote authentication provider . . . 14
Logging in to Nexus Dashboard using MFA . . . 15
Configure identity provider details . . . 16
Register your application . . . 16
Create client secret . . . 17
Configure API permissions . . . 17
Configure application manifest . . . 17
Configure directory extension attributes . . . 18
Assign extension attributes . . . 20
Configure claims mapping . . . 22
Multi-cluster primary as an authentication domain . . . 24
Guidelines and limitations . . . 24
Onboard multi-cluster and enable primary cluster to act as an authentication domain . . . 24
Enable primary cluster to act as an authentication domain and create multi-cluster login domain manually . . . 25
Log in using a multi-cluster domain . . . 25
Users . . . 27
Guidelines and limitations: Users . . . 27
Add local users . . . 27
Edit local users . . . 28
View remote user information . . . 28
Remote authentication . . . 29
Configure a remote authentication server . . . 29
Add LDAP as the remote authentication provider . . . 30
Add Radius or TACACS as the remote authentication provider . . . 32
Edit remote authentication domains . . . 33

Delete remote authentication domains . . . 33
Security . . . 34
Platform security and hardening enhancements . . . 34
Requirement for strong passwords . . . 34
User lockout . . . 35
Host list to access management interface . . . 35
Webserver security configuration . . . 36
SSH configuration . . . 37
Violation action . . . 38
Modify Violation action settings . . . 38
Security domains . . . 41
Create a security domain . . . 41
JWT keys . . . 42
Create a JWT key . . . 42
Credentials store . . . 42
Add a credentials store . . . 42
Validate peer certificates . . . 43
Export a certificate chain from Cisco APIC . . . 43
Import certificates into Nexus Dashboard . . . 45
Login banner . . . 45
Modify login banner text . . . 46
Add a proxy server . . . 47
Guidelines and limitations: Kerberos proxy authentication . . . 47
Copyright . . . 50

New and changed information

The following table provides an overview of the significant changes up to this current release. The table does not provide an exhaustive list of all changes or of the new features up to this release.

Release Version	Feature	Description
Nexus Dashboard 4.3.1	Ability to disable mandatory password change on first login	Beginning with this release, 'super-admin' users can use the **Mandatory password change on first login** field to disable mandatory password change on first login. For more information, see Violation action.
Nexus Dashboard 4.3.1	Device Upgrade Administrator	Beginning with Nexus Dashboard 4.3.1, the **Device Upgrade Administrator** role is reintroduced for device upgrade workflows in fabric software. This role was previously available as **NDFC Device Upgrade Admin**. For more information, see Roles and permissions in the unified releases.

Roles and permissions

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.

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.

These sections describe the user roles available in Nexus Dashboard and their associated permissions within the platform. 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.

- Understanding roles and permissions before and after the unified product
- Roles and permissions in the unified releases
- Mapping roles from non-unified releases

Understanding roles and permissions before and after the unified product

Prior to Nexus Dashboard release 4.1, there were roles provided at the Nexus Dashboard level and in the services running in Nexus Dashboard. For Nexus Dashboard release 4.1 (the first unified release) and later, the platform and the individual services are unified into a single product.

Roles and permissions in the unified releases

These are the roles and permissions in the unified releases (Nexus Dashboard release 4.1 and later).

User role	AV pair value	Description
Super Administrator	super-admin	Users with this role have full access to all resources in every security domain. A user with this role can perform all operations on the Nexus Dashboard, including backup and restore processes.
Fabric Administrator	fabric-admin	Users with this role have permissions for full fabric management, including creation of network policies, interface configurations and software upgrades. Users with this role and the all security domain access can also add and delete fabrics, including ACI fabrics, to a Nexus Dashboard cluster. See Connecting Clusters for more information.

User role	AV pair value	Description
Device Upgrade Administrator	device-upg-admin	Users with this role can perform device upgrade operations in fabric software, such as uploading switch firmware images, managing update groups, preparing and installing software updates, and viewing update logs and reports. This role was previously available as **NDFC Device Upgrade Admin**. Users with this role can also perform upgrade-related device actions, such as deleting files from switch bootflash, changing a switch between normal and maintenance modes, reloading switches, and running **show** commands. To perform device image upgrades, users with this role must be assigned the **Device Upgrade Administrator** role for the security domain associated with the target fabric, and they must be associated with the system-created all-tenants-domain tenant domain. The all-tenants-domain tenant domain provides access to all current and future tenants.
Designer	designer	Users with this role can make changes to the configuration (the intent) but cannot deploy those changes to the network fabrics.
Approver	approver	When change control is enabled, users with this role can perform operations related to the approval or denial of submitted configuration changes.
Observer	observer	Primarily a read-only user.
Support Engineer	support-engineer	Users with this role are able to perform tasks related to support, such as collecting tech support, creating backups, deploying templates, and general troubleshooting. When change control is enabled, users with this role can also deploy and revert policy changes that were approved. Users with this role are not able to make configuration changes.

Mapping roles from non-unified releases

This section provides information on mapping roles from non-unified releases (releases prior to Nexus Dashboard release 4.1) to the roles in the unified releases (Nexus Dashboard release 4.1 and later).



The Insights service did not support RBAC (any account that could log in to the Nexus Dashboard had full access to Insights), so there is no role-mapping

information from previous releases for Insights.

- Mapping Nexus Dashboard and Orchestrator roles
- Mapping Nexus Dashboard Fabric Controller roles

Mapping Nexus Dashboard and Orchestrator roles

User Role in Non-Unified Releases	User Role in Unified Releases
admin (read-only)	Observer
Administrator	Super Administrator
Approver	Approver
Dashboard User	Observer
Deployer	Support Engineer
Power-User	Super Administrator
Site Administrator	Fabric Administrator
Site Manager	Designer
Tenant Manager	Designer
User Manager	Super Administrator

Mapping Nexus Dashboard Fabric Controller roles

User Role in Non-Unified Releases	User Role in Unified Releases
NDFC Access Admin	Fabric Administrator
NDFC Change Approver	Approver
NDFC Change Deployer	Support Engineer
NDFC Device Upgrade Admin	Device Upgrade Administrator
NDFC Network Admin	Fabric Administrator
NDFC Network Operator	Observer
NDFC Network Stager	Designer

Choosing a 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. For more information, see Remote authentication.

1. Choose the default login domain.
   a. From the main navigation menu, select **Admin > Users and Security**.
   b. Click the **Authentication** tab.
   c. In the top right of the **Default authentication** tile, click the **Edit** icon.

      The **Edit default authentication** page opens.
2. In the **Edit default authentication** page that opens, choose the **Login domain** from the dropdown, then click **Save**.

Multi-factor authentication

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 Configure an Okta account as an MFA provider
- You will establish MFA provider and client integration, as described in Configure an MFA client.
- You will add the MFA provider as an external authentication domain in Nexus Dashboard, as described in Add Okta as a remote authentication provider.

Add Okta as a remote authentication provider

Before you begin

- You must have at least one user already configured in Okta as described in Configure an Okta account as an 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 Configure an Okta account as an MFA provider.
- If you want to use a proxy to connect to your Okta account, the proxy must already be configured as described in Add a proxy server.

To add Okta as a remote authentication provider:

1. Add an authentication domain.
    a. From the main navigation menu, select **Admin > Users and Security**.
    b. Click the **Authentication** tab.
    c. In the main pane, click **Create login domain**.
2. 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.
3. Click **Save** 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 that you created in Add Okta as a 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 Configure an Okta account as an 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.

Configure an Okta account as an 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

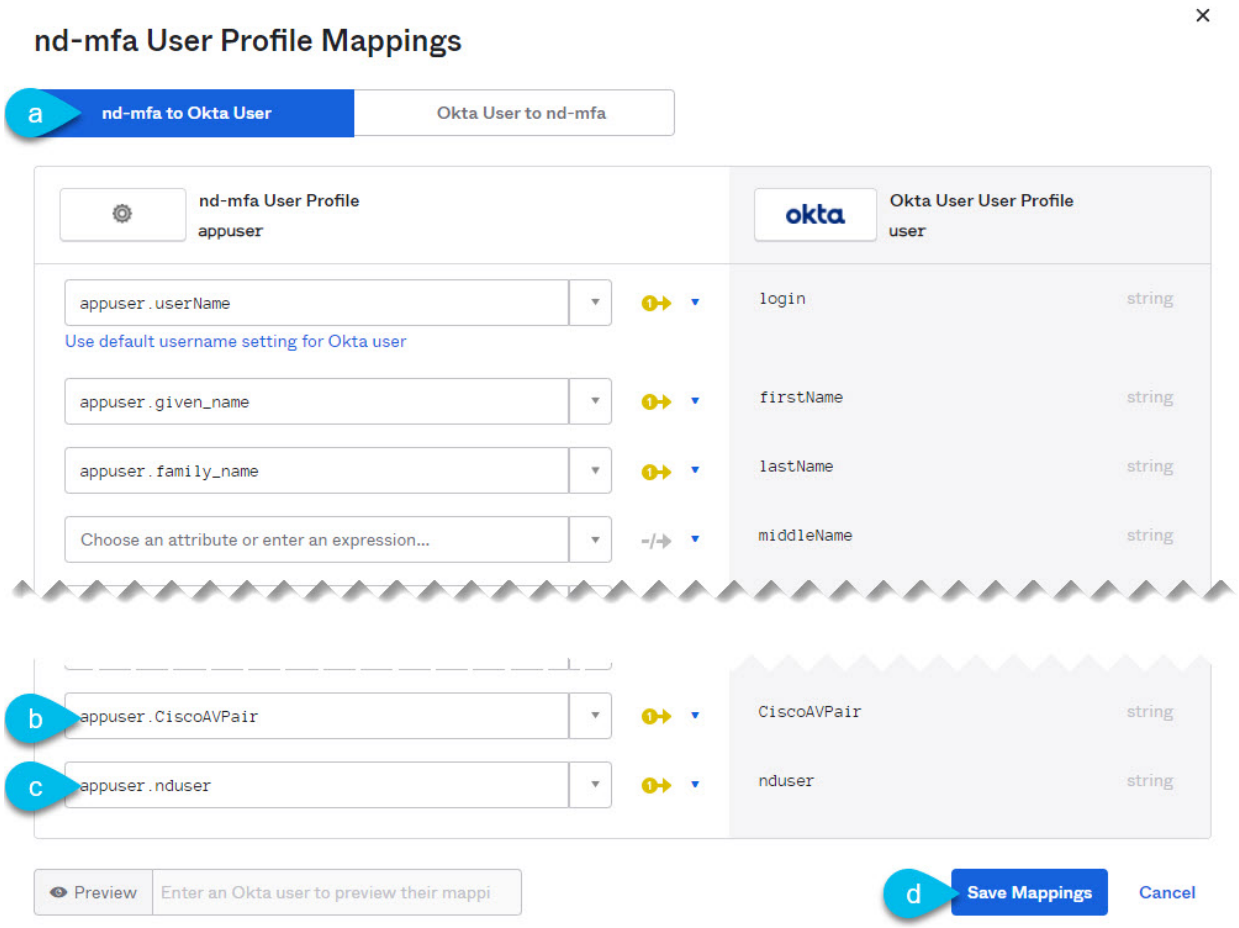
      Replace the <nd-node1-ip> with your cluster node IP address, then click **+Add URI** to provide the URIs for all nodes in the cluster.

   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 page, click **Mappings**.

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



d. At the top of the **nd-mfa User Profile Mappings** page, 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** page opens.

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

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

The **CiscoAVPair** values are described in the Configure a remote authentication server, for example shell:domains=all/super-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.

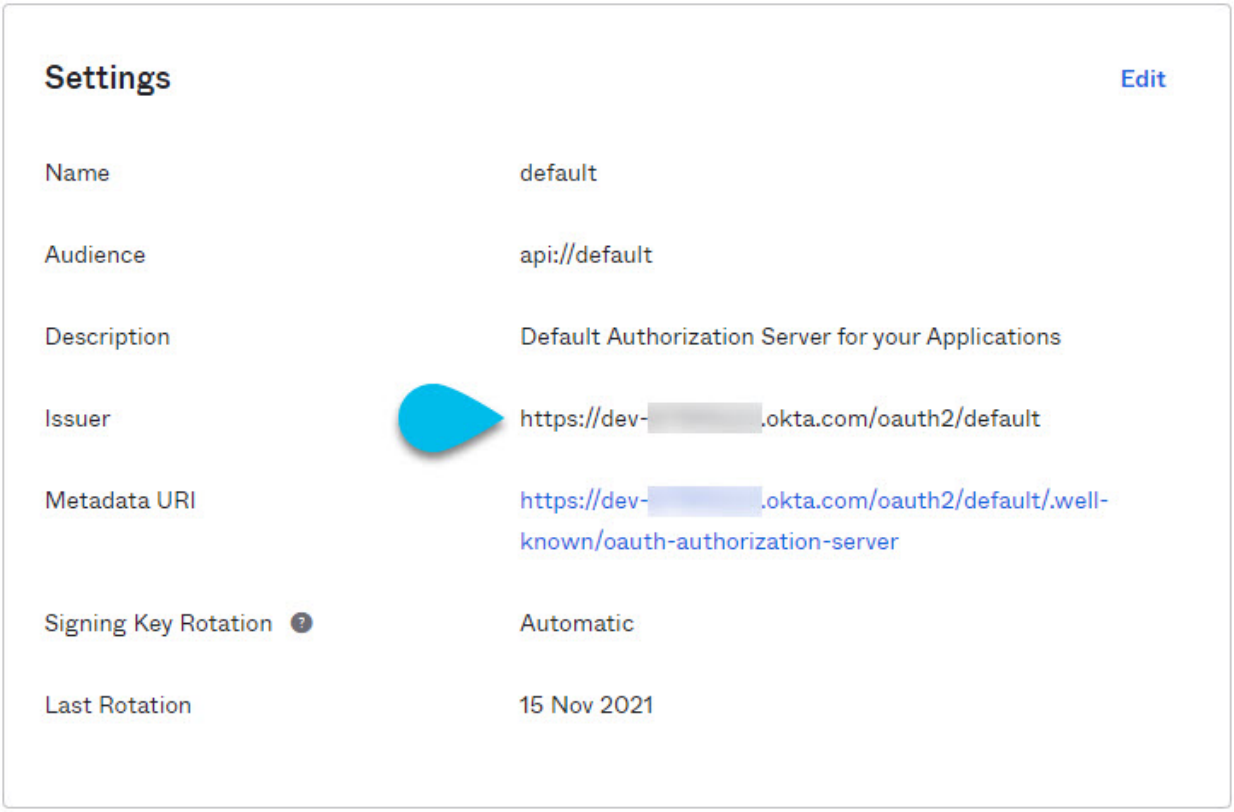
m. Click **Save**.

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.

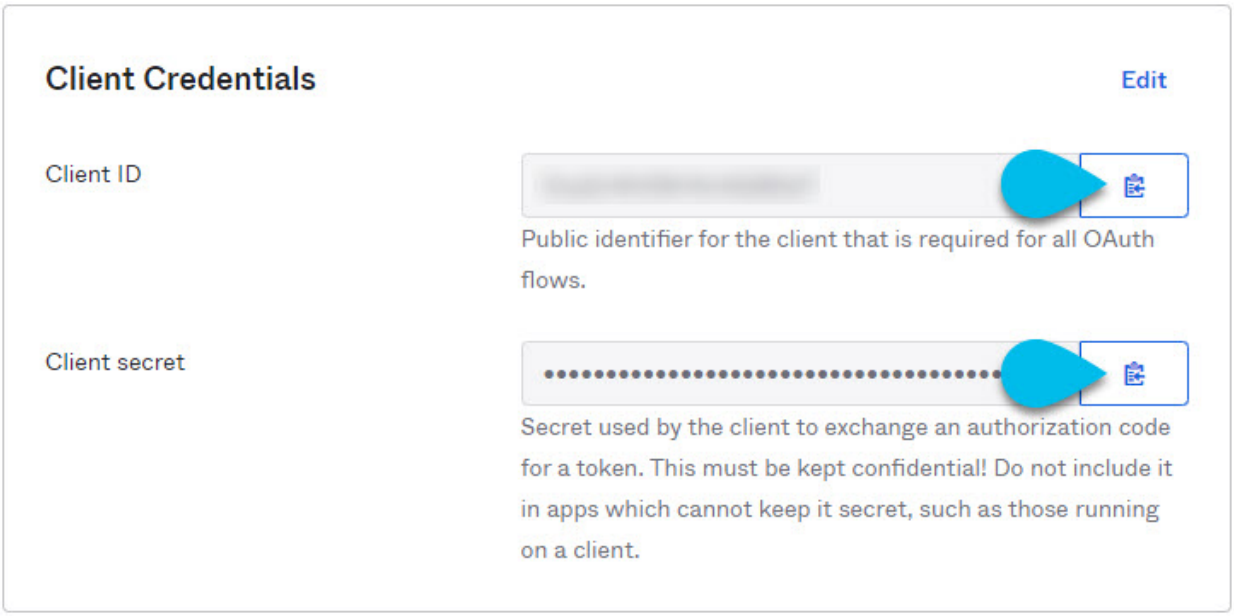
c. Note down the **Issuer** value.



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.



Configure an 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** page, 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.

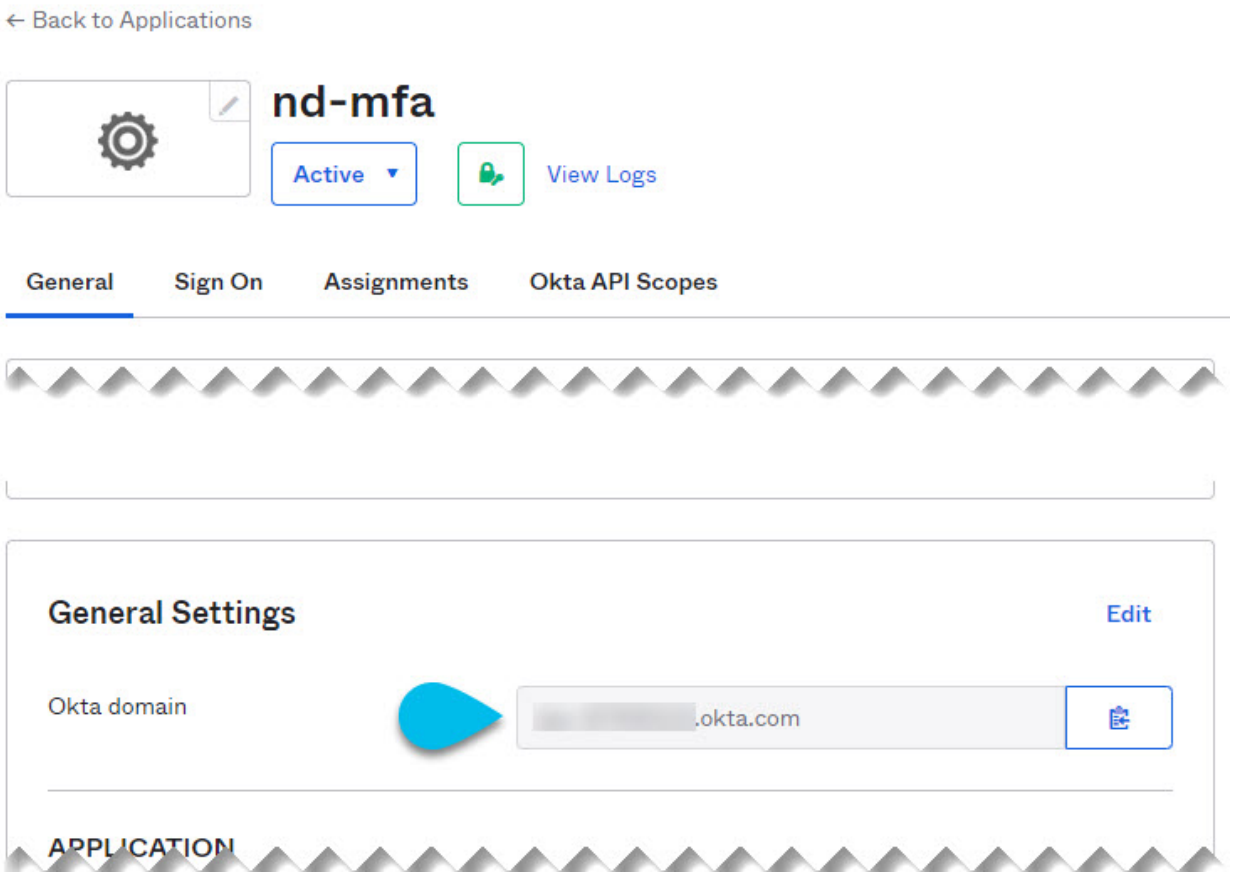
   To configure users in Duo dashboard:

   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 Configure an Okta account as an 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.

Microsoft Entra ID multi-factor authentication (MFA)

You can now configure Microsoft Entra ID multi-factor authentication (MFA) to enable users to log in with their Microsoft Entra ID credentials.

Nexus Dashboard uses the OpenID Connect (OIDC) authorization protocol to configure Microsoft Entra ID as an identity provider (IdP) for login and user authentication. Using the OIDC authentication protocol, Nexus Dashboard ensures secure handling of user credentials and provides a standardized way for identity verification across different applications.

Guidelines and limitations

- These Microsoft Entra ID (Azure Portal) permissions are required:
  - Application Administrator role OR Cloud Application Administrator role
  - User Administrator role is required to create and configure app registrations and to create directory extension attributes

Add Microsoft Entra ID as a remote authentication provider

Before you begin

- Register Nexus Dashboard as an application in Microsoft Entra ID. See Register your application.
- Configure OIDC parameters such as Client ID and Client Secret (from Entra ID) Create client secret.
- Redirect URI (where Entra ID sends the authentication token) Configure API permissions Configure API permissions.
- Configure your application with the Idp. See Configure application manifest.
- Ensure custom user attributes are added. See Configure directory extension attributes.
- Populate attributes with actual extension values. See Assign extension attributes.
- Configure values to be retrieved as part of claims mapping. See Configure claims mapping.

Follow these steps to add Microsoft Entra as a remote authentication provider.

1. Add a proxy server.
   a. Navigate to **Admin > System Settings > General**.
   b. In the **Proxy configuration** area, click **Edit**.
   c. Click **+ Add proxy server** in the proxy configuration page.
   d. From the **Type** drop-down list, choose **HTTP**.
   e. In the **Server** field, provide the full address for the proxy server, including the port if required.

      For example, http://proxy.company.com:80.

f. Click **Save**.

g. Click **+ Add proxy server** to add a secondary proxy server.

h. From the **Type** drop-down list, choose **HTTPS**.

i. In the **Server** field, provide the full address for the proxy server, including the port if required.

For example, http://proxy.company.com:80.

j. Click **Save**.

2. Add an authentication domain.

a. From the main navigation menu, choose **Admin > Users and Security**.

b. Click the **Authentication** tab.

c. Click **Create login domain**.

d. In the **Create login domain** page, provide domain details.

e. Provide the **Name** for the domain, for example, Entra.

f. (Optional) Provide a **Description** of the domain.

g. Click the **Realm** drop-down list, choose **Microsoft Entra Id**.

h. In the **Client ID** field, enter the client ID you obtained from your Microsoft Entra account.

i. In the **Client Secret** field, enter the client secret you obtained from your Microsoft Entra account.

j. In the **Issuer** field, enter the URL you obtained from your Microsoft Entra account. You can retrieve this from the **Overview > Endpoint** page from the Azure portal using the app registration used for Entra ID. You can copy and paste the OpenID Connect metadata document endpoint and remove the '.well-known/openid-configuration' from the URL.

k. Check the **User Proxy** option if you want to connect to Microsoft Entra over a proxy.

l. Leave the **Scopes** options unchecked.

m. Click **Save** to save the domain information and return to the **Admin > Users and Security > Authentication** page.

You should see an entry for the domain you created. For example, if you used "Entra" as your domain name, you will see a domain listed by this name in the **Name** column of the table.

3. Click the domain name listed in the Name column to view the details and verify all the information is correct.

4. Click **Refresh** on the **Admin > Users and Security > Authentication** page.

Logging in to Nexus Dashboard using MFA

Follow these steps to login to Nexus Dashboard using MFA.

1. Navigate to one of your Nexus Dashboard IPs as you typically would.

2. From the **Login Domain** drop-down list, choose the **Microsoft Entra Id** domain that you created in Add Microsoft Entra ID as a remote authentication provider.

The **Username** and **Password** fields will not be displayed.

3. Click **Login**.

   You will be redirected to the Microsoft Entra login page.

4. In the **Pick an account** dialog box, choose an ND account you created.
5. Enter a password for this account.
6. Click **Sign in**.

   A push notification will be sent to your Duo client.

7. Approve the login using Duo client.

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

Configure identity provider details

The following sections provide details on the configuration required to enable MFA for Nexus Dashboard using Microsoft Entra ID as an identity provider.

Register your application

Follow these steps to register your application.

1. Navigate to the Azure Portal https://portal.azure.com and sign in with your admin account.
2. Navigate to **Azure Active Directory > App registrations > + New registration**
3. Configure these settings.
   - Name: Nexus-Dashboard-OIDC (or your preferred name)
   - Supported account types: Select Accounts in this organizational directory only (Single tenant)
   - Redirect URI:
   - Platform: Web
   - URI: https://<node-management-ip>/oidccallback

     Example: https://198.51.100.1/oidccallback

     Administrators must add a redirect URI for every applicable cluster node in the following format:

     ```
     https://<node-1-management-ip>/oidccallback
     https://<node-2-management-ip>/oidccallback
     https://<node-n-management-ip>/oidccallback
     ```

4. Click **Register**.



After registration, you must save Application (client) ID, Directory (tenant) ID, and the Object ID information from the overview page.

Create client secret

Follow these steps to create a client secret.

1. In your app registration, navigate to **Manage > Certificates & secrets > Client secrets > + New client secret**
2. Add a description and expiry date:
   - **Description**: ND-OIDC-Secret
   - **Expires**: Choose an appropriate expiration time (6 months, 12 months, or 24 months)
3. Click **Add**
4. Save the **Secret Value**



Copy the **Secret Value** immediately and store it securely.

Configure API permissions

Follow these steps to configure the API permissions.

1. Navigate to the **API permissions > + Add a permission** page.
2. Choose **Microsoft Graph > Delegated permissions**.
3. Search for the User and add these from the search result.
   - **User.Read** (should already be there)
   - **User.ReadWrite.All** (needed for user attribute updates)
4. Click **Add permissions**.
5. Grant **Admin Consent**.
6. Click " Grant admin consent for [Your Organization]" .
7. Click **Yes** to confirm.
8. Verify all permissions show “Granted for [Your Organization]”.

Configure application manifest

Follow these steps to configure application manifest.

1. Edit Manifest. Navigate to the Manifest in your app registration.
2. Enable mapped claims.
   a. Find the line: " acceptMappedClaims" : null and change it to " acceptMappedClaims" : true.

   For example:

```
" api" : {
   " acceptMappedClaims" : true,
   " knownClientApplications" : [],
```

```
    "requestedAccessTokenVersion" : null,
    "oauth2PermissionScopes" : [],
    "preAuthorizedApplications" : []
}
```

3. Click **Save** at the top to save the Manifest.

Configure directory extension attributes

Directory extension attributes are custom attributes that store the user's Nexus Dashboard username and role information.

Create Extension Attributes via Azure CLI

1. Open Azure Cloud Shell
   - In Azure Portal, click the **Cloud Shell** icon (>_) at the top
   - Or go to: https://shell.azure.com
   - Choose **Bash** environment
2. Get **Application Object ID** Replace YOUR_CLIENT_ID with your Application (client) ID:

```
az rest --method GET \
  --uri "https://graph.microsoft.com/v1.0/applications?$filter=appId eq 'YOUR_CLIENT_ID'"

Example:

az rest --method GET \
  --uri "https://graph.microsoft.com/v1.0/applications?$filter=appId eq 'cf6303f8-3220-4351-99a7-727fcc92acc8'"
```

   - From the response, note the "id" field (this is the Object ID).

Create 'nduser' extension attribute

Replace YOUR_OBJECT_ID with the Object ID from the previous step:

```
az rest --method POST \
  --uri
```

```
" https://graph.microsoft.com/v1.0/applications/YOUR_OBJECT_ID/extensionProperties"  \

 --headers " Content-Type=application/json"  \

 --body '{

  " name" : " nduser" ,

 " dataType" : " String" ,

  " targetObjects" : [" User" ]

}'
```



Note down the returned " name" field (for example extension_cf6303f83220435199a7727fcc92acc8_nduser)

Create CiscoAVPair extension attribute

```
az rest --method POST \

 --uri
" https://graph.microsoft.com/v1.0/applications/YOUR_OBJECT_ID/extensionProperties"  \

 --headers " Content-Type=application/json"  \

 --body '{

  " name" : " CiscoAVPair" ,

  " dataType" : " String" ,

  " targetObjects" : [" User" ]

}'
```



The returned " name" field (For example, extension_cf6303f83220435199a7727fcc92acc8_CiscoAVPair)

Verify extension attributes

```
az rest --method GET \

 --uri
```

```
" https://graph.microsoft.com/v1.0/applications/YOUR_OBJECT_ID/extensionProperties"
```

You should see both **nduser** and **CiscoAVPair** attributes.

Assign extension attributes

You can assign extension attributes and set the values for different user roles.



You must have a user administrator role to perform this task.

Follow these steps to assign extension attributes.

1. Get User Object ID. Replace username with the user's display name or UPN:

```
az rest --method GET \
  --uri " https://graph.microsoft.com/v1.0/users?$filter=displayName eq 'username'"
```

```
Example:
az rest --method GET \
  --uri " https://graph.microsoft.com/v1.0/users?\$filter=displayName eq 'john.doe'"
```



Note the " id" field from the response (user's Object ID)

2. Set User Attributes Replace:
   a. USER_OBJECT_ID with the user's Object ID
   b. YOUR_CLIENT_ID_NO_DASHES with your Client ID (remove all dashes)
   c. username with the desired ND username
   d. ROLE with the appropriate role

```
az rest --method PATCH \
  --uri " https://graph.microsoft.com/v1.0/users/USER_OBJECT_ID" \
  --headers " Content-Type=application/json" \
  --body '{
    " extension_YOUR_CLIENT_ID_NO_DASHES_nduser" : " username" ,
    " extension_YOUR_CLIENT_ID_NO_DASHES_CiscoAVPair" : " shell:domains=all/ROLE"
  }'
```

Example for an Observer:

```
az rest --method PATCH \
  --uri " https://graph.microsoft.com/v1.0/users/95cc90b7-be2d-43b2-973e-
47a7bce6c9bc" \
```

```
  --headers "Content-Type=application/json"  \
  --body '{
    "extension_cf6303f83220435199a7727fcc92acc8_nduser": "john.doe",
    "extension_cf6303f83220435199a7727fcc92acc8_CiscoAVPair":
"shell:domains=all/observer"
  }'
```

Example for a Super Admin:

```
az rest --method PATCH \
  --uri "https://graph.microsoft.com/v1.0/users/fe3e5ae2-cae7-45fa-b169-
a398442cb309"  \
  --headers "Content-Type=application/json"  \
  --body '{
    "extension_cf6303f83220435199a7727fcc92acc8_nduser": "admin.user",
    "extension_cf6303f83220435199a7727fcc92acc8_CiscoAVPair":
"shell:domains=all/super-admin"
  }'
```

Example for Mixed Roles:

```
az rest --method PATCH \
  --uri "https://graph.microsoft.com/v1.0/users/a3ef6357-7f75-450c-b0e1-
9fb5e76b2583"  \
  --headers "Content-Type=application/json"  \
  --body '{
    "extension_cf6303f83220435199a7727fcc92acc8_nduser": "mixed.user",
    "extension_cf6303f83220435199a7727fcc92acc8_CiscoAVPair":
"shell:domains=all/observer|approver|fabric-admin"
  }'
```

Verify User Attributes

```
az rest --method GET \
  --uri
"https://graph.microsoft.com/v1.0/users/USER_OBJECT_ID?\$select=displayName,userPrin
cipalName,extension_YOUR_CLIENT_ID_NO_DASHES_nduser,extension_YOUR_CLIENT_ID
_NO_DASHES_CiscoAVPair"
```

You should see the **nduser** and **CiscoAVPair** values in the response

Configure claims mapping

1. Navigate to your Enterprise Application.
   a. **Azure Portal > Azure Active Directory > Enterprise applications**
   b. Search for your application and choose your application. For example, Nexus-Dashboard-OIDC.
2. Access Single Sign-On settings
   a. In the left menu, click **Single sign-on**.
   b. Under **Attributes & Claims**, click **Edit**.
3. Add new claims
   a. Add **CiscoAVPair** claim.
      i. Click **+ Add new claim**.
         - **Name**: CiscoAVPair .
         - **Source**: Choose **Directory schema extension** . A popup will appear with "Select Application" message.
      ii. In the search box, enter your application name, for example, Nexus-Dashboard-OIDC.
      iii. Choose your application, for example, Nexus-Dashboard-EntraID-Dev. This application should have your Client ID.
      iv. Click **Select**. A popup appears with a message that says, "Add Extension Attributes" . You will see a list of available extension attributes:

      user.CiscoAVPair (extension_cf6303f8...)

      user.nduser (extension_cf6303f8...)

      v. Choose user.CiscoAVPair.
      vi. Click Add. The Schema extension attribute field will be populated with the full extension name
      vii. Click Save.
   b. Add **nduser** claim:
   c. Click **+ Add new claim**
      - **Name**: nduser
      - **Source**: Select **Directory schema extension**. A popup will appear with a message that says, "Select Application" .
   d. Search for your application and select it. For example, *Nexus-Dashboard-EntraID-Dev *.
   e. Click **Select**.
   f. In the “Add Extension Attributes” popup, choose **user.nduser**
   g. Click **Add**. The **Schema extension attribute** field will be populated

h. Click **Save**.

4. Verify claims configuration.
   a. You should now see two additional claims in the list:
      - **Claim name**: CiscoAVPair, **Type**: JWT, **Value**: user.ciscoavpair (extensi...)
      - **Claim name**: nduser, **Type**: JWT, **Value**: user.nduser (extension_cf...)



You may see an information banner: “OIDC Applications require custom signing keys to customize claims.” If you encounter issues, expand **Advanced settings** and ensure acceptMappedClaims is enabled.

Multi-cluster primary as an authentication domain

In Nexus Dashboard, you can configure the primary cluster as the authentication domain to support role-based access control (RBAC) across clusters, eliminating the need for a an external authentication provider, such as a AAA remote authentication server. Local users (with observer role) configured on the primary cluster can login as remote users from any clusters with a login domain in Multi-cluster realm type. For more information, see Log in using a multi-cluster domain.



A cluster can have only one multi-cluster authentication login domain of the Multi-cluster realm type.

You can create a multi-cluster login domain in Nexus Dashboard during onboarding. You can check the **Enable multi-cluster authentication domain** check box and provide a name for the multi-cluster login domain. For more information on creating multi-cluster login domain, see Onboard multi-cluster and enable primary cluster to act as an authentication domain.

Guidelines and limitations

- When you enable a multi-cluster domain and provide a login name during creation (greenfield), the login domain is created for both primary and secondary clusters.
- If you enable the multi-cluster domain during a subsequent onboarding, the login domain is created in the primary cluster and only on the new secondary cluster being onboarded. You must manually create the domain for all other secondary clusters.
- If a multi-cluster domain login already exists during onboarding, attempting to create it using the **Enable multi-cluster authentication domain** check box will result in no action.
- Upgrades from previous Nexus Dashboard releases require manually creating a multi-cluster domain login. For example, if you are upgrading from Nexus Dashboard 3.2 to 4.3.1, you can manually create a multi-cluster domain login to use this feature. For more information, see Enable primary cluster to act as an authentication domain and create multi-cluster login domain manually
- Disabling the multi-cluster domain login on a secondary cluster affects only that cluster, while disabling it on the primary cluster affects all clusters.

Onboard multi-cluster and enable primary cluster to act as an authentication domain

Follow these steps to onboard multi-cluster and enable primary cluster to act as an authentication domain.

1. Log in to the Nexus Dashboard of the cluster to designate it as the primary cluster.
2. Add the second cluster.
3. Navigate to **Admin > System Settings**.
4. Click **Multi-cluster connectivity**.
5. Click **Connect Cluster**.

6. In **Select type**, choose **Nexus Dashboard**.
7. Click **Next**.
8. In the Remote cluster settings page, enter these field values:
    a. **Hostname IP Address**
    b. **Username**
    c. **Password**
    d. **Login domain**
9. Check the **Enable multi-cluster authentication domain** check box.
10. Enter a name for **Multi-cluster login domain name**, for example, MulticlusterAuth.
11. Click **Next** to connect the clusters.

Enable primary cluster to act as an authentication domain and create multi-cluster login domain manually

Follow these steps to enable primary cluster to act as an authentication domain and create multi-cluster login domain manually.

1. From the main navigation menu, choose **Admin > Users and Security**.
2. Click the **Authentication** tab.
3. Check the check box next to the multi-cluster domain you created.
4. Choose **Actions > Create login domain**.
5. In the **Create login domain**, provide domain details.
    a. Provide the **Name** for the domain.
    b. (Optional) Add a description for the domain **Description**.
    c. From the **Realm** drop-down list, choose Multi-cluster realm type.
6. Check the **Enable multi-cluster authentication domain** check box.
7. Click **Save**

    You can use the **Actions** drop-down list to perform these actions.

    - Choose **Actions > Set as default** to set the multi-cluster domain as the default authentication provider.
    - Choose **Actions > Edit** to make changes to the login domain information.
    - Choose **Actions > Delete** to delete the multi-cluster domain.

Log in using a multi-cluster domain

Follow these steps to log in using a multi-cluster domain.

1. Navigate to one of your Nexus Dashboard IP addresses.
2. Enter your username and password in the **Username** and **Password** fields.

3. From the **Login Domain** drop-down list, choose multi-cluster domain name you created. For example, Multi-cluster domain.
4. Click **Login**.

Users

The **Users** 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.

Guidelines and limitations: Users

- The default local observer 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.
- When an administrator adds a local user as described in Add local users, the administrator must provide a password for that local user. When that local user then logs into the Nexus Dashboard for the first time, they will be asked to change their password again at that initial login stage. If the **Mandatory password change on first login is enabled**, see Violation action for more information.
- When configuring local users, note that all local user configurations are case sensitive.

Add local users

1. Create a new local user.
    a. From the main navigation menu, select **Admin > Users and Security**.
    b. Click the **Users** tab.
    c. In the main pane, click **Create local user**.
2. In the **Create local user** screen that opens, provide user details.
    a. Provide the **User ID** that will be used for logging in.
    b. Provide and confirm the initial **Password**.

    As described in Guidelines and limitations: Users, when the local user that is being created in these procedures first logs into the Nexus Dashboard, they will be asked to change their password again at that initial login stage.

    c. Provide the **First Name**, **Last Name**, and **Email** for the user.
    d. Determine if you want to set the **Remote user authentication** field to **Enabled** or **Disabled**.

    Remote user authentication is used for signing into Nexus Dashboard when using identity providers that cannot provide authorization claims. If you choose **Enabled** for this **Remote user authentication** field, the local user ID can't be used to directly log in to the Nexus Dashboard.

    e. Provide the **Remote ID claim** information.
    f. Click **+ Add Security Domain and Roles**.
    g. In the **Security Domain Name** field, choose the security domain to associate with this user.
    h. In the **Role** field, choose the role to associate with this user.

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.

i. Choose the tenant domain to associate with this local user in the **Tenant domain** field, if applicable.

The **Tenant domain** field is displayed if the tenant or tenant group functionality that is introduced in Nexus Dashboard release 4.2.1 is enabled. For more information, see Configuring Tenants and Tenant Domains.

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

Edit local users

1. Open user details screen.
   a. From the main navigation menu, select **Admin > Users and Security**.
   b. Click the **Users** tab.
   c. In the main pane, click on the user's name.
   d. In the details pane that opens, click the **Details** icon.
2. In the ***<user-name>*** details screen that opens, click the **Edit** icon.
3. In the **Edit User** screen that opens, update the settings as necessary.



If you choose the **Reset password** option for this local user, a password security workflow is enforced, similar to the one described in Add local users, where this local user will be asked to change their password again at that initial login stage when they first log into the Nexus Dashboard. The **Reset password** option is only valid when editing a local user.

View remote user information

To view remote users:

1. From the main navigation menu, select **Admin > Users and Security**.
2. Choose **Users > Remote**.

   If you use remote authentication for TACACS or RADIUS, those remote users will appear on this page after their first login to Nexus Dashboard with their remote credentials.

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 observer for the Nexus Dashboard cluster will also have admin privileges in the APIC.

Configure a 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. See Roles and permissions in the unified releases for a list of the Nexus Dashboard user roles and the AV pair you would use to define the roles on a remote authentication server, such as LDAP.

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

```
shell:domains=<domain1>/<Role1>|<Role2>,<domain2>/<Role2>|<Role3>
```

For example, the following string illustrates how to assign the Observer role to a user in all domains, and the Fabric Administrator role in domain_A:

```
shell:domains=all/observer,domain_A/fabric-admin
```

Add LDAP as the remote authentication provider

Before you begin

- You must have at least one user already configured on the LDAP server as described in Configure a 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. Add an authentication domain.
   a. From the main navigation menu, select **Admin > Users and Security**.
   b. Click the **Authentication** tab.
   c. In the main pane, click **Create login domain**.
2. 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** page opens.
3. 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=observer, 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.

4. (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** page 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.

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

Add Radius or TACACS as the remote authentication provider



Beginning with 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 remote authentication server as described in Configure a 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. Add an authentication domain.
   a. From the main navigation menu, select **Admin > Users and Security**.
   b. Click the **Authentication** tab.
   c. In the main pane, click **Create login domain**.
2. 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** page opens.
3. 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. 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.

4. Click **Save** to finish adding the domain.

Edit remote authentication domains

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

1. From the main navigation menu, select **Admin > Users and Security**.
2. Click the **Authentication** tab.
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.

Delete remote authentication domains

1. From the main navigation menu, select **Admin > Users and Security**.
2. Click the **Authentication** tab.
3. From the **Actions** menu for the domain, select **Delete Login Domain**.
4. In the **Confirm Delete** prompt, click **OK** to confirm.

Security

The **Security** page allows you to view and manage certificates used by Nexus Dashboard. To access the **Security** page, navigate to **Admin > Users and Security > Security**.

Use these tabs to configure security in this page:

- Webserver security configuration
- SSH configuration
- Violation action
- Security domains
- JWT keys
- Credentials store
- Login banner

Platform security and hardening enhancements

Beginning with Nexus Dashboard 4.2.1, security on Nexus Dashboard has been enhanced.

These include:

- stronger password checks and password expiry
- user lockout after repeated failed login attempts
- host list to access management interface
- SSH enhancements such as idle timeout configuration and enabling or disabling SSH, and
- audit log enhancements.

Requirement for strong passwords

- A new security enhancement is now implemented where local users are required to change their password in these situations:
  - When the local user logs into Nexus Dashboard for the first time after they are added to the system
  - If the configuration information for the local user is edited and the **Reset password** option is enabled through this process:
    - Navigate to **Admin > Users and Security > Users**.
    - Choose the local user and click **Actions > Edit local user**.
    - Enable **Reset password** and click **Save**.
- Nexus Dashboard enforces the following enhanced password checks:
  - The username and password cannot be the same.
  - The username cannot be part of the password. This is case insensitive. For example, if the username is *Johndoe*, then a password like *!johnDoe1* is not accepted as it contains the username.

- The password must include a combination of at least 3 lower case letters, upper case letters, numbers, and special characters. However, the same character cannot be used more than four times in a consecutively.

  Four or more consecutive characters in the English alphabet or the **QWERTY** keyboard cannot be used in the password. This check for consecutive characters is applicable for both directions (left to right and right to left) in the English alphabet and the English keyboard.

- The last five passwords cannot be reused. This number can be configured from **Violation action > Reuse restriction limit**.

  For more information, see the Violation action section in *Exploring Your Nexus Dashboard*.

- You can also modify these settings related to password security for Nexus Dashboard:
  - Set the minimum password length
  - Enable enforcement of stricter password checks
  - Set the duration after which a local password expires

User lockout

You can also configure the number of consecutive failed login attempts and the user lockout time. By default, only the Nexus Dashboard GUI user **admin** and the SSH **rescue-user** are unlocked after the lockout time.

All other users who are locked out must be unblocked manually. This setting can be modified to allow all GUI users to be unblocked after the timeout.

However, the SSH rescue-user can not be unblocked manually. This user can only be unlocked after the lockout duration expires.

For more information, see the Violation action section in *Exploring Your Nexus Dashboard*.

Host list to access management interface

Designated IP addresses can be added, removed, and updated in the Nexus Dashboard for administrative terminals. This IP address restriction for management access applies to HTTPS, SSH and Rest APIs.

You can configure a designated list of host IP addresses, the allowed list of hosts, to access the webserver. The SSH user can be accessed through the management IP address.

You can add, remove, or update the list of hosts in the Nexus Dashboard from **Admin > Users** and the **Security > Security** menu. This list of hosts can access the webserver and SSH rescue-user on the Nexus Dashboard. By default, all hosts have access privileges, while the configured allowed list restricts access only to configured hosts. The webserver and SSH rescue-user allowed lists are configured independently.



This allowed list of hosts is not available to data center interfaces as it may directly interfere with the basic functionality of the system and the management of managed devices.

Webserver security configuration

The **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)

  For information about generating these files for self-signed certificates, see the "Generating a private key and self-signed certificate" section in Managing Certificates in your Nexus Dashboard.

- 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 Backing Up and Restoring Your Nexus Dashboard.

To edit security configuration:

1. Edit security configuration.
   a. From the main navigation menu, select **Admin > Users and Security**.
   b. Click the **Security** tab.
   c. In the main pane, click the **Security configuration** tab.
   d. In the main pane, click the **Edit** icon.
2. In the **Edit security configuration** screen that opens, update one or more fields as required:

   You need to paste the information in the following fields since uploading the keys and certificate files is not supported.

   a. Update the **Session timeout**.

      Specifies the duration for all HTTP sessions (GUI and API) with the default duration set to 20 minutes.

   b. In the **Domain name** field, provide your domain.
   c. Check the box in the **Minimum TSL version: TLSV1.3** field if you want to set the minimum SSL version to TLSV1.3.

      The minimum SSL version is set to TLSV1.2 by default. Checking this box to set the minimum version to TLSV1.3 will reject all clients using a TLSV1.2 connection request.

   d. To disable Qualtrics integration from the browser at a system wide level, check the box in the **Enforce strict content security policy** field.

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 algorithms (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.

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

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

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

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

e. Click **Save** to save the changes. **Add Allowed Subnet** content is not added in the **Webserver security configuration** tab.

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

SSH configuration

The **SSH configuration** page shows:

- the session idle timeout which can be pre-configured in Nexus Dashboard to 1800 seconds. SSH sessions connected to the management interface (SSH rescue-user) exceeding this idle timeout duration will be terminated.
- the option to enable or disable SSH on the management interface on Nexus Dashboard. SSH cannot be disabled for the data center interfaces.
  - The service port 22 on the management interface is closed when the SSH service is disabled.

Follow these steps to edit the information provided in the **SSH configuration** page.

1. From the main navigation menu, select **Admin > Users and Security**.
2. Click the **Security** tab.
3. In the main pane, click the **SSH configuration** tab.

   The current settings for these login actions are displayed in the **Management and Data interfaces SSH configurations** area.

   - Data center interface SSH configuration
     - Ciphers
     - Host key algorithms
     - MACs
     - Key Exchange algorithms
   - Management interface SSH configuration
     - Session timeout (seconds)
     - Ciphers

        - Host key algorithms
        - SSH connection
        - MACs
    - Key Exchange algorithms
4. If you want to change any of the above settings, click **Edit**.
5. To configure allowed subnet, click **Add allowed subnet** and specify the IPv4 or IPv6 address and mask.
6. Click **Save**.

Violation action

The **Violation action** page shows the number of unsuccessful attempted login actions. The login actions that you configure through the **Violation action** page apply to actions and users that are configured through the Webserver security configuration and SSH configuration pages.

Nexus Dashboard enforced a mandatory password change for users logging in for the first time, with no option to disable this setting. In Nexus Dashboard release 4.3.1, 'super-admin' users can use the **Mandatory password change on first login** field to disable mandatory password change on first login. The **Mandatory password change on first login** option is enabled by default. When this option is enabled, new users or users whose passwords were reset by the super-admin must go through a mandatory password change.

Modify Violation action settings

Follow these steps to modify the information provided in the **Violation action** page.

1. Navigate to **Admin > Users and Security**.
2. Click the **Security** tab.
3. In the main pane, click the **Violation action** tab.

   The current settings for these login actions are displayed in the **Login action** area.

    - Maximum failed login attempts
    - Duration unlock
    - Lock duration for general user
    - Lock duration for UI admin user and SSH rescue user
    - Minimum password length
    - Strong password check
    - Reuse restriction limit
    - Password expiry duration
4. If you want to change the settings for any of these login actions, click **Edit**.

   The **Login action** page appears.

5. Change the settings in any of these login actions, if necessary.

Field	Description
Maximum login attempts	Set the maximum number of login attempts in the **Count** field until the violation action is triggered. The default entry is 0, which represents unlimited login attempts.

Field	Description

Number of failed attempts before user is locked out	Set the violation action if the maximum number of login attempts is reached in the **Lock for a configured duration** field, where a locked login is unlocked after a certain duration or through a default admin user-assisted unlock. The default admin user and SSH rescue user is subjected to a duration-based unlock only.
	
	• **OFF** (the default setting): With this setting, only the admin user and SSH rescue user has a duration-based unlock.
	  ◦ In the **Lock duration for UI admin user and SSH rescue user** area, set the amount of time, in seconds, minutes, or hours, that a login block will take place for an admin user and SSH rescue user when the number of maximum login attempts has been surpassed. Default entry for this field is 300 seconds.
	
	  When the violation action is triggered based on the maximum number of login attempts set in the **Maximum login attempts** area, the admin user and SSH rescue user has a duration-based unlock, where they are locked out for the duration set in the **Lock duration for UI admin user and SSH rescue user**.
	
	  ◦ All users other than the admin/SSH rescue user (in other words, general users) do not have a duration-based unlock and must be unlocked manually only by users with a super-admin role. Users with roles other than a super-admin role cannot unlock users that are locked out.
	• **ON**: With this setting, both the admin/SSH rescue user and any other (general) users have a duration-based unlock.
	  ◦ In the **Lock duration for UI admin user and SSH rescue user** area, set the amount of time, in seconds, minutes, or hours, that a login block will take place for an admin user and SSH rescue user when the number of maximum login attempts has been surpassed. Default entry for this field is 300 seconds.
	
	  When the violation action is triggered based on the maximum number of login attempts set in the **Maximum login attempts** area, the admin user and SSH rescue user has a duration-based unlock, where they are locked out for the duration set in the **Lock duration for UI admin user and SSH rescue user**.
	
	  ◦ In the **Lock duration for general user** area, set the amount of time, in seconds, minutes, or hours, that a login block will take place for a general user when the number of maximum login attempts has been surpassed. Default entry for this field is 1200 seconds.
	
	  When the violation action is triggered based on the maximum number of login attempts set in the **Maximum login attempts** area, the general user has a duration-based unlock, where they are locked out for the duration set in the **Lock duration for general user**.

Field	Description
Minimum password length	Set the minimum password length in the **Length** field. Default entry is 8.
Strong password check	Set the strong password check enforcement. • Disabled (the default setting): Strong password check enforcement is not enforced. • Enabled: Strong password check enforcement is enforced.
Mandatory password change on first login	Use the togglq to enable or disable mandatory password change on first login. When enabled, users must change their password the first time they login.
Reuse restriction limit	Prevents the reuse of a certain number of last-used passwords. Enter the number of last-used passwords that can be reused in the **Count** field. • A reuse limitation of 1 only blocks reusing the current password. • Default entry is 5.
Password expiry	Specifies the time duration in days after which a local user password expires, which requires the user to change the password before logging in. Enter a value in the **Password expiry duration (days)** field. A value of 0 indicates that the password expiry is not enabled. Default entry is 0.

6. Click **Save**.

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.

Create a security domain

Follow these steps to create a security domain.

1. Navigate to **Admin > Users and Security**.
2. Click the **Security** tab.
3. In the main pane, click the **Security domains** tab.

4. In the main pane, click **Create security domain**.
5. In the **Create security domain** screen that opens, provide the domain details.
6. Provide the **Name** for the domain.
7. (Optional) Provide a description for the domain.
8. Click **Save** to save the domain.

JWT keys

Create a JWT key

Follow these steps to create a JWT key.

1. Navigate to **Admin > Users and Security**.
2. Click the **Security** tab.
3. In the main pane, click the **JWT keys** tab.
4. Click **Create JWT key**.

   The **Create JWT key** page appears.

5. Enter a service name for the JWT key in the **Service name** field.
6. Enter a JWT API key in the **JWT API key** field.
7. Enter a JWT public key in the **JWT public key** field.
8. Enter the remote ID claim information in the **Remote ID claim** field.
9. Click **Create**.

Credentials store

You can add an external Credentials store that allows you to store and retrieve network credentials from an external vault, such as the CyberArk vault, instead of a local storage system.

Add a credentials store

Follow these steps to add a credentials store.

1. Navigate to **Admin > Users and Security**.
2. Click the **Security** tab.
3. In the main pane, click the **Credentials store** tab.
4. Click **Add credential store**.

   The **Edit credential store** page appears.

5. In the **Store type** field, choose a store type, such as CyberArk.
6. Enter the necessary information in the remaining fields, depending on the choice that you made in the **Store type** field.

For example, if you chose CyberArk in the **Store type** field, make the necessary choices in the following fields:

- In the **CyberArk CCP URL** field, enter the CyberArk Central Credential Provider (CCP) URL.

  For more information, see Central Credential Provider (CCP).

- In the **Certificate name** field, choose the appropriate certificate from the dropdown list.

  The **Certificate name** field lists the certificates that you configured in **Admin > Certificate Management**.

  > Ensure that the system certificate you configured is mapped to the CyberArk feature to use the certificate name here.

  For more information on system certificates, see Managing Certificates in your Nexus Dashboard.

7. Click **Resync/Save**.

> - Credentials retrieved from CyberArk are cached by the Nexus Dashboard credential management service. If there is a password change in CyberArk, whether automatically or manually, Nexus Dashboard will require approximately 10 minutes to reflect the updated password. To retrieve the updated password, navigate to the **Credential Store** and perform a **Resync**.
> - For SAN fabrics, credential store integration applies to Cisco MDS and Fibre Channel (FC) switch workflows.

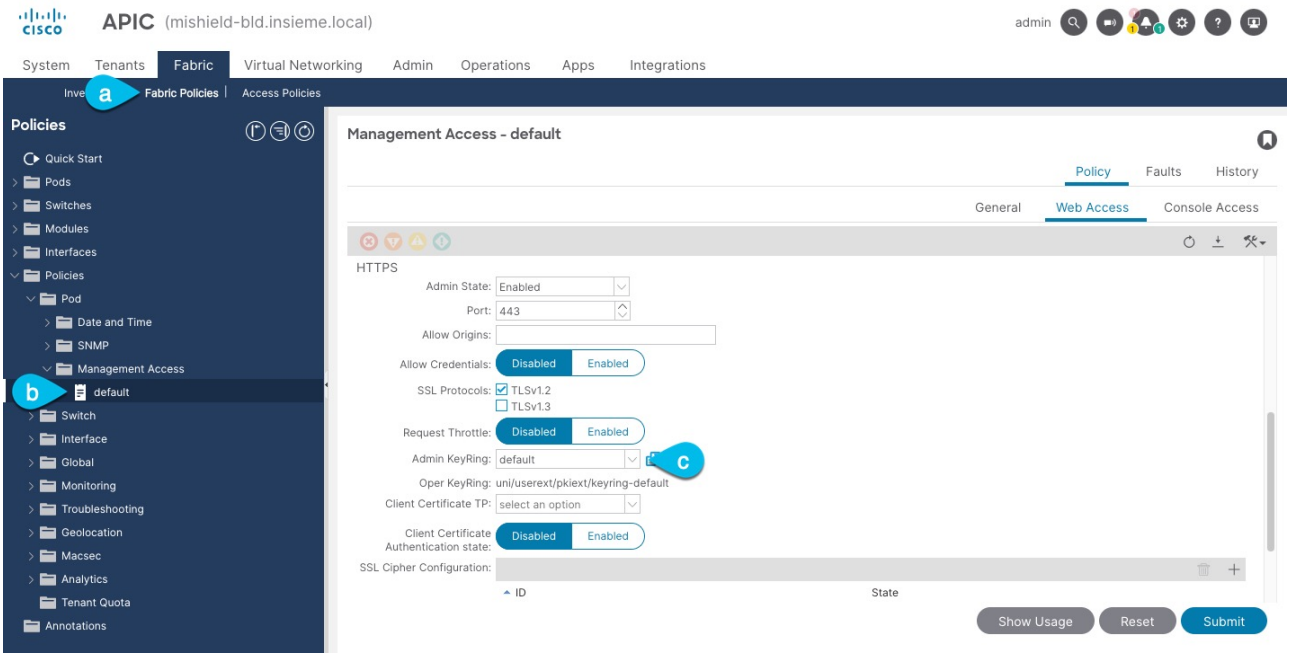
Validate peer certificates

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.

Export a certificate chain from Cisco APIC

Follow these steps to export a 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**.

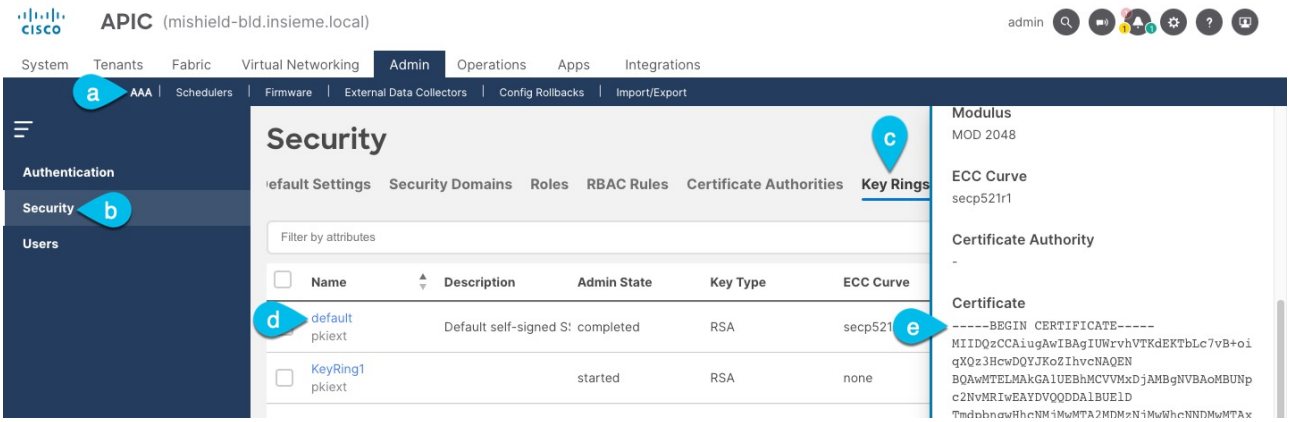
b. In the left navigation menu, choose **Policies > Pod> Management Access**.

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-----
```

Import certificates into Nexus Dashboard

Follow these steps to import certificates into Nexus Dashboard.

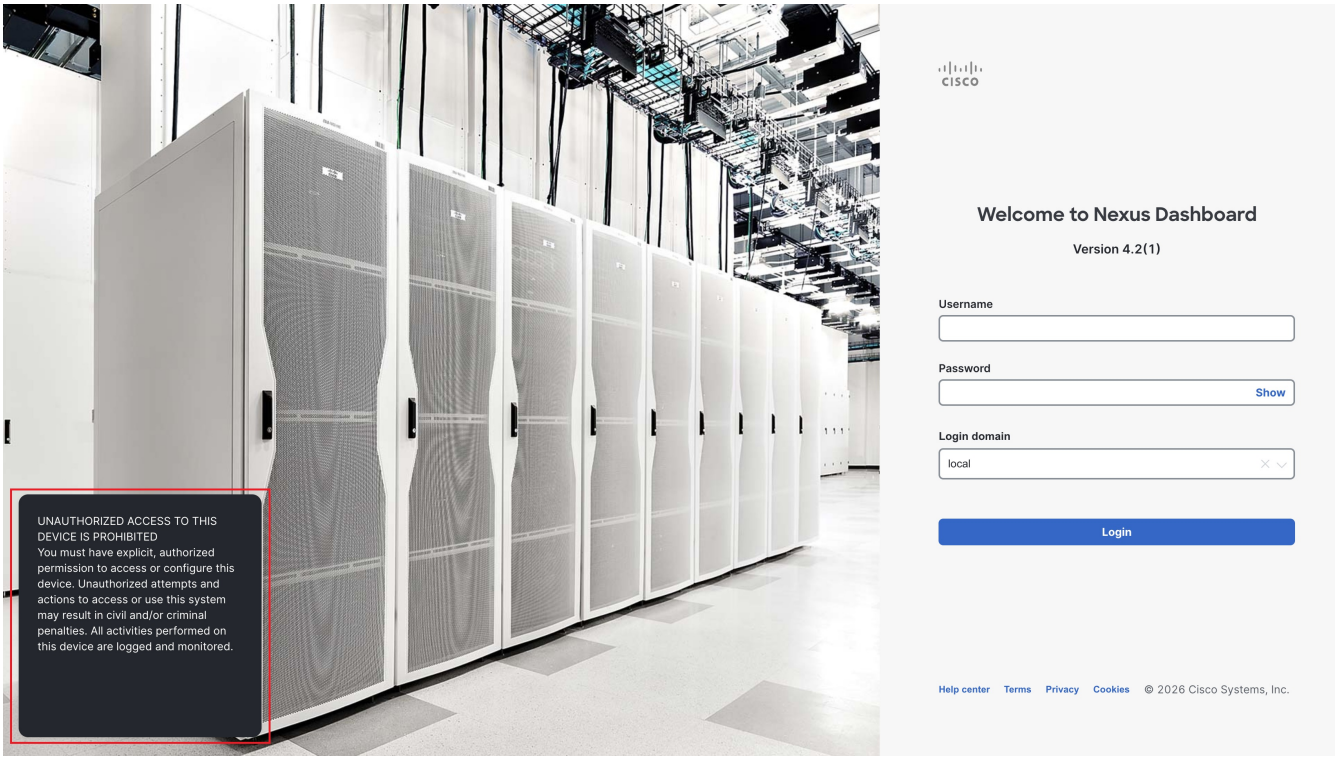
1. Log in to your Nexus Dashboard where you plan to onboard the fabrics.
2. Import the certificate into Nexus Dashboard.
    a. Log in to your Nexus Dashboard where you will onboard the fabrics.
    b. From the main navigation menu, select **Admin > Certificate Management**.
    c. Click the **CA Certificates** 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 Creating Fabrics and Fabric Groups.

Login banner

A super-admin user can modify the text that appears in the lower left corner of the login page. You can modify this text to announce planned outages, to share important system messages, or to show a legal disclaimer.



Modify login banner text

Follow these steps to modify login banner text.

1. From the main navigation menu, click **Admin > Users and Security**.
2. Click **Login banner**.

   The text that currently appears when you log into your Nexus Dashboard is shown in the **Login banner** area.

3. Click **Edit**.
4. Change the text that is currently used in the login banner, then click **Save**.

You will now see the new login banner text the next time you log into your Nexus Dashboard.

Add a proxy server

In certain deployment scenarios, you may have to access the Internet through a proxy.

Note that Nexus Dashboard uses two main route tables—one for the Management network and one for the Data network—and by default, it will use the routing table of the originating IP address. In other words, Nexus Dashboard will attempt to reach the proxy from the routing table of the POD/Service that is trying to use the proxy.

For example, if you configure a proxy and establish Intersight connectivity from your Nexus Dashboard and then attempt to configure the AppDynamics integration from the Insights service running in the cluster, you may get an error stating that the AppDynamics host is not reachable. This happens because the proxy is only accessible from the management interface, so in such cases you also need to add a management network route for the proxy IP address.

Beginning with Nexus Dashboard release 4.3.1, you can configure Kerberos-based authentication for outbound proxy traffic. In earlier releases, Nexus Dashboard supported only proxy configurations that used no authentication or username and password authentication.

With Kerberos proxy authentication, Nexus Dashboard acts as a Kerberos client. Nexus Dashboard authenticates to your organization's Key Distribution Center (KDC), obtains the required Kerberos tickets, and uses those tickets to authenticate to the configured proxy for all outbound HTTP and HTTPS traffic.

Kerberos proxy authentication applies only to outbound Nexus Dashboard traffic to the configured HTTP or HTTPS proxy. Nexus Dashboard does not use Kerberos to authenticate users or to authenticate directly to destination websites or services.

Before you begin

- Ensure that the proxy is configured to support Kerberos authentication.
- Ensure that Nexus Dashboard can reach the Kerberos Key Distribution Center (KDC).
- Ensure that time is synchronized between Nexus Dashboard and the KDC.

Guidelines and limitations: Kerberos proxy authentication

- Nexus Dashboard supports only one Kerberos realm for proxy authentication. You cannot configure multiple realms or domain-realm mappings.
- Nexus Dashboard manages runtime Kerberos tickets. These tickets are not user-configurable.
- Kerberos relies on time-sensitive tickets. Time skew between Nexus Dashboard and the KDC can cause authentication failures. Ensure that both systems use the same NTP source.
- The configured KDC and proxy server must be compatible with the Nexus Dashboard cluster networking mode:
  - In an IPv4-only deployment, Nexus Dashboard rejects IPv6-only values.
  - In an IPv6-only deployment, Nexus Dashboard rejects IPv4-only values.
  - In a dual-stack deployment, Nexus Dashboard allows either IPv4 or IPv6 values.

- The Kerberos password is stored securely in the Credential Management Service (CMS). Runtime Kerberos tickets (TGT and TGS) are transient and are not backed up, restored, or preserved across a restart or upgrade. After a restart, upgrade, or restore, Nexus Dashboard automatically reacquires fresh tickets by using the stored credentials.
- If Kerberos ticket acquisition fails after you save the configuration, Nexus Dashboard raises a system anomaly. For information about viewing system anomalies, see View platform and system alerts in global anomalies table.

Follow these steps to add a proxy server.

1. Navigate to **Admin > System Settings > General**.
2. In the **Proxy configuration** area, click **Edit**.
3. Click **+ Add proxy server** in the **Proxy Configuration** page.

   To configure Kerberos authentication for an existing proxy server, click the edit icon for the proxy entry. To replace an existing proxy configuration, delete an existing proxy entry and then click **+ Add proxy server**.

4. From the **Type** dropdown, select the type of traffic that you want to be proxied.

   If you choose **HTTP** and **HTTPS**, Nexus Dashboard applies the same proxy configuration to both HTTP and HTTPS traffic.

5. In the **Server** field, provide the full address for the proxy server, including the port if required.

   For example http://proxy.company.com:80.

   You can specify the proxy server as a hostname, IPv4 address, or IPv6 address. If you specify the proxy server as an IP address, the Kerberos environment must support an IP-based service principal name (SPN) for the proxy.

6. Choose the required authentication type:
   - None
   - Credentials
   - Kerberos
7. If you choose Credentials, provide the **Username** and **Password**.
8. If you choose **Kerberos**, add the Kerberos realm.
   a. In the **Realm** area, click **+ Add realm**.
   b. In the **Add Realm** page, provide the realm details:

Field	Description
Name	Kerberos realm name.
KDC	Hostname, IPv4 address, or IPv6 address of the Kerberos KDC.
Username	Username that Nexus Dashboard uses to authenticate to the KDC.
Password	Password for the Kerberos username.

c. Click **Save**.

9. (Optional) In the **Client principal name** field, enter the Kerberos client principal.

   If you do not provide a value, Nexus Dashboard generates the client principal from the username and realm.

10. (Optional) In the **Service principal name** field, enter the Kerberos service principal for the proxy.

    If you do not provide a value, Nexus Dashboard generates the service principal from the proxy server hostname and realm.

11. Click **Save**.

    Nexus Dashboard saves the Kerberos proxy configuration only after it successfully validates the KDC and acquires the required Kerberos tickets. After validation succeeds, Nexus Dashboard displays the validation status and the time of the last successful validation.

12. (Optional) Click **+ Add Ignore Host** to provide any hosts that bypass the proxy.

    You can add one or more hosts that the cluster communicates with directly, bypassing the proxy.

13. Click **Save**.

    Nexus Dashboard records proxy configuration changes in the audit logs.

Copyright

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.

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

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: https://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)

© 2017-2026 Cisco Systems, Inc. All rights reserved.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706

USA
https://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883