Managing Your Device Credentials, Release 4.2.1

Table of Contents

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 4.2.1	There were no major changes from the previous release.	

Managing your device credentials

While changing the device configuration, Nexus Dashboard uses the device credentials provided by you. However, if you do not provide the LAN switch credentials, Nexus Dashboard prompts you to open the **Manage** > **Device Credentials** page to configure the LAN credentials.

Nexus Dashboard uses two sets of credentials to connect to the LAN devices:

- **Discovery Credentials**

  Nexus Dashboard uses these credentials during discovery and periodic polling of the devices.

  Nexus Dashboard uses discovery credentials with SSH and SNMPv3 to discover the hardware or software inventory from the switches. You can discover one inventory per switch. These discovery credentials are read-only and you cannot make configuration changes on the switches.

- **Configuration Change Credentials**

  Nexus Dashboard uses these credentials when a user changes the device configuration.

LAN Credentials

You can use the write option on the LAN credentials page to do configuration changes on the switch. One credential is allowed per user for a single switch. A user role must access Nexus Dashboard to use the write option for the switches to push configurations on it through an SSH connection.

For a user role created on NX-OS switches, an SNMPv3 user is created with the same password. Ensure that the SSH and SNMPv3 credentials match for the discovery of the credentials. If SNMP authentication fails, discovery of credentials stops displaying an error message. If SNMP authentication succeeds and SSH authentication fails, discovery of credentials continues, and the switch status displays a warning message for the SSH error.

If the user role created on the NX-OS switches uses AAA authentication, the SNMPv3 user is not created. Using this AAA authentication to discover or import a switch in Nexus Dashboard, the controller detects that the local SNMPv3 user is not created on the switch. Nexus Dashboard runs the exec command on the switch to create an SNMPv3 user with the same password on the switch. The SNMPv3 user role is temporary. Once the user role expires, the continual discovery of switches from Nexus Dashboard creates the SNMPv3 user.

LAN credentials management allows you to specify configuration-change credentials. Before changing any LAN switch configuration, you must enter the LAN credentials for the switch. If you do not provide the credentials, the configuration change action is rejected.

These features get the device-write credentials from the LAN credentials feature.

- Upgrade (ISSU)
- Maintenance mode (GIR)
- Patch (SMU)
- Template deployment
- POAP-write erase reload, rollback

- Interface creation, deletion, or configuration
- VLAN creation, deletion, or configuration
- VPC wizard

You must specify the configuration-change credentials irrespective of whether the devices were discovered initially or not. This is a one-time operation. After the credentials are set, the credentials are used for any configuration-change operation.

Default Credentials

You use default credentials to connect all the devices that the user has access to. You can override the default credentials by specifying credentials for each of the devices in the **Devices** table.

Nexus Dashboard tries to use individual switch credentials in the devices, to begin with. If the credentials (username/password) columns are empty in the devices, the default credentials are used.

Robot Credentials

When you specify default credentials, you can enable the robot feature, enabling the robot flag.

The robot user role helps with switch and device accounting. You can track all the changes done on Nexus Dashboard with a general user account. If the user role changes on Nexus Dashboard that impacts the change on the device, this is termed an out-of-band change.

These changes are logged on the device as the changes made by a general user account. Therefore, you can track and distinguish between out-of-band changes and changes made on the device. This general user account is termed as a robot user role for the changes logged on the device.

For example, a user role of network-admin on Nexus Dashboard has access to enter LAN device credentials to push configurations on the switches. With the network-admin user role, you can check the robot flag while creating the LAN credentials.

The username for the LAN credentials is displayed as a change logged on the device. If a username for the LAN credentials is changed to a controller and the robot flag is checked, the credentials for the device changes from default to robot.

This user role pushes configurations on the switches in Nexus Dashboard. These changes are logged in the **History** tab of the fabric as the changes made by the network-admin user role. The account log on the switch displays as the controller. The appropriate user-role details are logged on Nexus Dashboard and the device.

In Nexus Dashboard, the robot user role is considered the admin role for all the fabrics and the devices. If the default credential is not set on a fabric, you can use the robot user role, if it is set for different devices.

If another user role with write access logs in to Nexus Dashboard, this user role is not prompted to update the credentials as the robot user role is already set. The credentials are set in the following order: individual switch, robot, and then the default credentials.

In the **LAN Credentials Management** page, you can choose to either use default credentials or robot credentials while changing device configurations, unless you set custom credentials.

To set the default credentials:

1. Navigate to the **LAN Credentials Management** page:

   Manage > Device Credentials

2. In the **Default Credentials** area, determine that status of the default credentials.
   - **Not Set**: The default credentials have not been set yet.
   - **Default Set**: The default credentials are being used when changing the device configuration, unless custom credentials are set for the devices in the table.
   - **Robot Set**: Robot credentials are being used when changing the device configuration, unless custom credentials are set for the devices in the table.
3. Change the default credentials, if necessary.
   a. In the **Default Credentials** area, click **Set**.

      The **Set Default Credentials** dialog box appears.

      You will see two tabs: **Local** and **Credential Store**.

      

      You will see the **Credential Store** tab only if you configured system certificate and mapped to CyberArk feature. For more information on CA certificates and credential store, see Managing Certificates in your Nexus Dashboard and Configuring Users and Security.

   b. If you haven't configured credential store, in the **Local** tab, enter the necessary username and password information.
   c. If you have configured credential store, in the **Credential Store** tab, enter the credential store key.
   d. Choose the **Robot** checkbox to set the robot credentials.

      

      If you enable the **Enable AAA passthrough of device credentials** feature under **Admin > System Settings > Fabric Management > Management**, then you cannot set the robot flag.

   e. Click **Save**.

      The status of the default credentials changes based on your selection.
4. To clear the default device credentials, click **Clear**.

   A confirmation message appears. Click **Clear Credentials** to clear the default device credentials.

To edit the credentials for a specific device:

1. Choose the required **Device Name** and click **Actions > Edit**.

   The **Edit Credentials** dialog box appears.
2. Enter the necessary username and password information, then click **Save**.

Switch Table

The **Devices** table lists all the LAN switches that the user has access to. You can specify the switch credentials individually, which will override the default credentials. In most cases, you need to provide only the default credentials.

The LAN credentials for the Nexus Dashboard **Devices** table has the following fields.

Field	Description
Device Name	Displays the switch name.
IP Address	Specifies the IP address of the switch.
Credentials	Specifies whether the default or switch-specific custom credentials are used.
Username	Specifies the username that Nexus Dashboard uses to login.
Fabric	Displays the fabric to which the switch belongs.

The following table describes the action items, in the **Actions** menu drop-down list, that appear on the **LAN Credentials Management** page.

Action Item	Description
Edit	Choose a device name and click **Edit**. Specify a username and password. You can edit local or custom- specific credentials.
Clear	Choose a device name and click **Clear**. A confirmation dialog box appears. Click **Yes** to clear the switch credentials from the Nexus Dashboard server.
Validate	Choose a device name and click **Validate**. A confirmation message appears, indicating if the operation was successful or a failure.

Copyright

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