Switches

Switches

The following table describes the fields that appear on **Switches** window.

Field	**Description**
Switch Name	Specifies name of the switch.
IP Address	Specifies IP address of the switch.
Fabric Name	Specifies the associated fabric name for the switch.
Status	Specifies the status of the switch.
Health	Specifies the health status of the switch. The following are health status: • Healthy • Critical • Warning • OK
Ports	Specifies the total number of ports on switch.
Used Ports	Specifies the total number of used ports on switch.
Model	Specifies the switch model.
Serial Number	Specifies the serial number of the switch.
Release	Specifies the release number of the switch.
Up Time	Specifies the switch up time details.

The following table describes the action items, in the Actions menu drop-down list, that appear on **SAN** > **Switches** > **Switches**.

Action Item	Description
Device Manager	You can log in to Device Manager for required switch. The **Device Manager** login window appears, enter credentials and log in. See Device Manager to view descriptions and instructions for using the Cisco MDS 9000 Device Manager.
Tech Support	Allows you to initiate log collection. For more information, see Tech Support, on page 2.
Execute CLI	Allows you to run multiple CLI commands on multiple switches and collect output as zipped text file for each switch. For more information, see Execute CLI, on page 2.

Device Manager

See Device Manager chapter for descriptions and instructions for using the Cisco MDS 9000 Device Manager.

Note Device Manger session is terminated when you navigate to another tab on the **Switch Overview** screen.

Tech Support

From the **Actions** drop-down list, select **Tech Support** to initiate log collection. A window appears.

- Enter time in **Session timeout** field in minutes, by default time is 20 minutes.
- Enter the command in **Command** text field and click **Run**.
- A confirmation window appears stating 'Data submitted successfully, tech support starting', click **Confirm** and status changes to **Completed**.
- You can download the report, click **Download Tech Support**.

Execute CLI

From Release 12.0.2f, Cisco NDFC SAN Controller allows you to execute CLI commands on switches. You can collect the output from the CLI commands in `.zip` file for each switch.

To execute CLI commands on switches, do the following:

1. On the Cisco NDFC UI, choose **SAN** > **Switches** > **Switches**.
2. Select the switches on which you want to execute the CLI commands.

   You can select more than one switch to run the set of CLI commands simultaneously.

3. From the **Actions** drop-down list, choose **Execute CLI** .

   The **Execute Switch CLI** screen is displayed.

4. On the **Configure** tab, click on the hyperlink under **Selected Switches** to view the selected switches on which the CLIs will be executed.

5. In the **CLI Commands** text box, enter the CLI commands to be executed on the switches.

   Ensure that you enter one command per line.

6. Click **Execute**.

   A **Success** confirmation message appears.

7. On the **Execute** tab, the tables displays switch, associated fabric and the CLI execution status.

8. Click on **Download output** to download the command output.

Note If switch is not reachable via CLI then the output in zip file will indicate an error.

Enhanced Role-based Access Control

Starting from SAN Controller Release 12.0.1(a), all RBAC is in Nexus Dashboard. User-roles and access are defined from Nexus Dashboard for fabrics on NDFC.

Nexus Dashboard admin role is considered as Network-admin role in NDFC.

DCNM had five roles to perform various access and operations. If a user is access a fabric with network stage role has access to all other fabrics as a network stage role. Therefore, a username is restricted with their role in DCNM.

Cisco NDFC Release 12.0.1(a) has same five roles but you can do granular RBAC with integration of Nexus Dashboard. If a user accesses a fabric as a network stage role, the same user can access different fabric with other user role such as admin or operator role. Therefore, a user can have different access on the different fabrics in NDFC.

NDFC RBAC supports following roles:

- NDFC Access Admin
- NDFC Device Upgrade Admin
- NDFC Network Admin
- NDFC Network Operator
- NDFC Network Stager

The following table describes the user roles and their privileges in NDFC.

Roles	**Privileges**
NDFC Access Admin	Read/Write See

Roles	Privileges
NDFC Device Upgrade Admin	Read/Write
NDFC Network Admin	Read/Write
NDFC Network Operator	Read
NDFC Network Stager	Read/Write

The following roles are supported on DCNM for backward compatibility:

- SAN admin (mapped to network-admin)
- Global-admin (mapped to network-admin)
- SAN network-admin (mapped to network-admin)
- Server-admin (mapped to network-admin)

Note In any window, the actions that are restricted by the user role that is logged in are grayed out.

NDFC Network Admin

A user with the **NDFC Network Admin** role can perform all the operations in SAN Controller.

You can freeze a particular fabric or all fabrics in SAN Controller if you are a user with the **NDFC Network Admin** role.

Note Make sure that the switch user role for discovery or add switches or LAN credentials for NDFC must have the network-admin role.

NDFC Device Upgrade Admin

A user with the **NDFC Device Upgrade Admin** role can perform operations only in **Image Management** window.

See the Image Management section for more information.

NDFC Access Admin

A user with the **NDFC Access Admin** role can perform operations only in **Interface Manager** window for all fabrics.

An NDFC access admin can perform the following actions:

- Add, edit, delete and deploy layer 2 port channels, and vPC.
- Edit host vPC, and ethernet interfaces.
- Save, preview, and deploy from management interfaces.

- Edit interfaces for LAN classic, and IPFM fabrics.

  Apart from nve, management, tunnel, subinterface, SVI, interface grouping, and loopback interfaces

However, a user with the SAN Controller access admin role can’t perform the following actions:

- Cannot edit layer 3 port channels, ST FEX, AA FEX, loopback interfaces, nve interfaces, and subinterfaces.
- Cannot edit member interfaces and port channels of Layer 3, ST FEX, AA FEX.
- Cannot edit interfaces with policy associated from underlay and link for easy fabrics.
- Cannot edit peer link port channel.
- Cannot edit management interface.
- Cannot edit tunnel.

Note The icons and buttons are grayed out for this role when the fabric or SAN Controller is in deployment-freeze mode.

NDFC Network Stager

A user with the **NDFC Network Stager** role can make configuration changes on SAN Controller. A user with the **NDFC Network Admin** role can deploy these changes later. A network stager can perform the following actions:

- Edit interface configurations
- View or edit policies
- Create interfaces
- Change fabric settings
- Edit or create templates

However, a network stager cannot perform the following actions:

- Cannot make any configuration deployments to switches.
- Cannot perform deployment-related actions from the SAN Controller Web UI or the REST APIs.
- Cannot access the administration options like licensing, creating more users, and so on.
- Cannot move switches in and out of maintenance mode.
- Cannot move fabrics in and out of deployment-freeze mode.
- Cannot install patches.
- Cannot upgrade switches.
- Cannot create or delete fabrics.
- Cannot import or delete switches.

NDFC Network Operator

A network operator can view fabric builder, fabric settings, preview configurations, policies, and templates. However, a network operator cannot perform the following actions:

- Cannot change expected configurations of any switch within any fabric.
- Cannot deploy any configurations to switches.
- Cannot access the administration options like licensing, creating more users, and so on.

The difference between a network operator and a network stager is that, as a network stager you can only define intent for existing fabrics, but cannot deploy those configurations.

Only a network admin can deploy the changes and edits that are staged by a user with the network stager role.

Choosing Default Authentication Domain

By default login screen on Nexus Dashboard chooses the local domain for authentication. You can change domain at login time by choosing available domains from drop-down list.

Nexus Dashboard supports local and remote authentication. The remote authentication providers for Nexus Dashboard include RADIUS, and TACACS. For more information on authentication support, refer https://www.cisco.com/c/en/us/td/docs/dcn/nd/2x/user-guide/cisco-nexus-dashboard-user-guide-211.pdf.

The following table describes RBAC comparison between DCNM and NDFC access:

DCNM 11.5(x)	NDFC 12.0.x and 12.1.x
• User has a single role. • All APIs and resources are accessed with this single role.	• User can have a different role in different Nexus Dashboard for sec domains. • Security domain contains single Nexus Dashboard, and each Ne Dashboard contains single NDFC Fabric.
A single role is associated with the user by disabling or restricting the access to options in DCNM.	A single role displays only privileged resources on the selected page restricted access are grayed out based on security domain associated selected resource on further options on NDFC.
DCNM AV Pair format with shells, roles, and optional access constraints.	Nexus Dashboard AV Pair format with shells, domains.
Supported roles based on deployment type LAN, SAN, or PMN.	Supported roles such as network-admin, network-operator, device-upg-admin, network-stager, access-admin are in NDFC. Support for legacy roles for backward compatibility. Nexus Dashboa admin role as network-admin of DCNM.

The following table describes DCNM 11.5(x) AV Pair format:

Cisco DCNM Role	RADIUS Cisco-AV-Pair Value	TACACS+ Shell Cisco-AV-Pair Value

Network-Operator	shell:roles = "network-operator"
	dcnm-access="group1 group2 group5"
		cisco-av-pair=shell:roles="network-operator
		dcnm-access="group1 group2 group5"

Network-Admin	shell:roles = "network-admin"
	dcnm-access="group1group2 group5"
		cisco-av-pair=shell:roles="network-admin"
		dcnm-access="group1 group2 group5"

The following table describes NDFC 12.x AV Pair format:

User Role	AVPair Value
NDFC Access Admin	Access-admin
NDFC Device Upgrade Admin	Device-upg-admin
NDFC Network Admin	Network-admin
NDFC Network Operator	Network-operator
NDFC Network Stager	Network-stager

The AV pair string format differs when configuring a read/write role, read-only role, or a combination of read/write and read-only roles for a specific user. A typical string includes the domain, followed by the read-write roles separated from the read-only roles using the slash (/) character; individual roles are separated by the pipe (|) character:

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

Nexus Dashboard Security Domains

Access control information about a user login contains authentication data like user ID, password, and so on. Based on the authorization data, you can access resources accordingly. Admins in Cisco Nexus Dashboard can create security domains and group various resource types, resource instance, and map them into a security domain. The admins define an AV-pair for each user, which defines the access privileges for users to different resources in Cisco Nexus Dashboard. When you create a fabric, a site is created in Nexus Dashboard with the same fabric name. You can create and view these sites from **Nexus Dashboard > Sites**.

The SAN Controller REST APIs use this information to perform any action by checking the authorization.

Note When accessing REST APIs, you can verify passed payload in JSON format. Ensure that the payload is an appropriate JSON format.

When you upgrade from SAN Controller Release 11.x, each fabric is mapped to an autogenerated site of the same name. All these sites are mapped into the **all** security domain in Nexus Dashboard.

All resources are placed in **all** domain before they are assigned or mapped to other domains. The all security domain does not include all the available security domains in Nexus Dashboard.

AV-Pairs

A group of security domains along with read and write roles for each domain are specified using AV-pairs. Administrators define AV-pair for each user. The AV-pair defines the access privileges to users across various resources in Nexus Dashboard.

The AV-pair format is as follows:

```
"avpair":
"shell:domains=security-domain/write-role-1|write-role-2,security-domain/write-role-1|write-role2/read-role-1|read-role-2"

For example: "avpair":
```

```
"shell:domains=all/network-admin/app-user|network-operator". "all/admin/" makes user
super-user and it's best to avoid examples with all/admin/"
```

The write role is inclusive of read role as well. Hence, `all/network-admin/` and `all/network-admin/network-admin` are the same.

Note From SAN Controller Release 12.0.1a supports the existing AV-pair format that you created in SAN Controller Release 11.x. However, if you are creating a new AV-pair, use the format that is mentioned above. Ensure that the shell: domains must not have any spaces.

Specifying Cisco NX-OS User Roles and SNMPv3 Parameters on AAA Servers

You can use the VSA cisco-AV-pair on AAA servers to specify user role mapping for the Cisco NX-OS device using this format:

```
shell:roles="roleA roleB …"
```

If you do not specify the role option in the cisco-AV-pair attribute, the default user role is network-operator.

You can also specify your SNMPv3 authentication and Privacy protocol attributes as follows:

```
shell:roles="roleA roleB..." snmpv3:auth=SHA priv=AES-128
```

The SNMPv3 authentication protocol options are SHA and MD5. The Privacy protocol options are AES-128 and DES. If you do not specify these options in the cisco-AV-pair attribute, MD5 and DES are the default authentication protocols.

Creating a Security Domain

To create a security domain from Cisco Nexus Dashboard, perform the following steps:

1. Log into Cisco Nexus Dashboard.
2. Choose **Administrative > Security**.
3. Navigate to **Security Domains** tab.
4. Click **Create Security Domain**.
5. Enter the required details and click **Create**.

Creating a User

To create a user from Cisco Nexus Dashboard, perform the following steps:

1. Log into Cisco Nexus Dashboard.
2. Choose **Administrative > Users**.
3. Click **Create Local User**.
4. Enter the required details and click **Add Security Domain**.
5. Choose a domain from the drop-down list.
6. Assign a SAN Controller service read or write role by checking the appropriate check box.

7. Click **Save**.

Switch Overview

UI Path: **SAN** > **Switches** > **Switch Overview**

The Switch Overview menu includes the following sub menus:

Viewing Switch Summary

You can view information about switch along with the switch summary on **Switch Overview** tab. Navigate **SAN** > **Switches**, click on required switch. A slide-in pane appears. Click **Launch** icon to view the **Switch Overview** window.

The following are the default cards that appear in the **Summary** tab:

Card	Description
Switch Information	Displays details of switch such as name, health status, IP address, model, version and other switch information.
Event Analytics	Displays events with **Critical**, **Major**, **Minor**, and **Warning** severity. In this card, click **Launch** icon to navigate to events tab for more information.
Resources	Displays the resource utilization of switch in the graph form.
Modules	Displays the switches on which the modules are discovered, the models name and the count.
Interfaces	Displays the switch interface summary information.
Port Usage	Displays the ports inventory summary information.

Modules

To view the inventory information for modules from the SAN Controller Web UI, perform the following steps:

Procedure

Step 1 Choose **SAN > Switch > Switch Overview > Modules**. Similarly you can view modules from fabric overview window, **SAN > Fabric > Fabric Overview > Modules**

The **Modules** tab is displayed with a list of all the switches and its details for a selected Scope.

You can view required information in table, enter details in **Filter by Attributes**.

Step 2 You can view the following information.

- **Name** displays the module name.
- **Model** displays the model name.
- **Serial Number** column displays the serial number.
- **Type** column displays the type of the module.
- **Oper. Status** column displays the operation status of the module.
- **Slot** column displays the slot number.
- **HW Revision** column displays the hardware version of the module.
- **Software Revision** column displays the software version of the module.
- **Asset ID** column displays the asset id of the module.

Viewing Interface

UI Path: **SAN** > **Switch** > **Switch Overview** > **Interface**

Similarly you can view interface on fabric overview window.

SAN > **Fabric** > **Fabric Overview** > **Interface**

The following table describes the fields that appear on the **Interfaces** tab.

Field	Description
Name	Specifies the interface name.
Admin. Status	Specifies the administration status of the interface.
Oper. Status	Specifies the operational status of the interface.
Reason	Specifies the reason for failure.
Speed	Specifies the speed of the interface in Gbs.
Mode	Specifies the mode of the interface.
Switch	Specifies the name of the switch.
VSAN	Specifies the name of the connected VSAN.
Connected To	Specifies the connection details.
Connected To Type	Specifies the type of connection.
Description	Specifies the details about the interface.
Owner	Specifies the port owner name.

Field	Description
Port Group	Specifies the port group number for the interface connected.

To perform various operations on the inventory tab, follow the below procedures:

Procedure

Step 1 To perform no shutdown for an interface, select the check box for the required interface and choose **Actions** > **No Shutdown**.

A warning window appears, click **Confirm**.

Step 2 To shutdown an interface, select the check box for the required interface and choose **Actions** > **Shutdown**.

A warning window appears, click **Confirm**.

Step 3 To assign a port owner for an interface, do the following:

a) Select the check box for the required interface and choose **Actions** > **Owner**.

b) In the **Set Port Owner** dialog box that appears, enter a required name and click **Apply**.

Step 4 To set up diagnostic for an interface, select the check box for the required interface and choose **Actions** > **Link Diagnostics**.

Viewing Switch Licenses

You can view the following information on Licenses tab.

- **Feature** column displays the feature names of the selected switch.
- **Status** column displays the status of licenses. Status will be either **In Use** or **Unused**.
- **Type** column displays the type of the licenses.
- **Warnings** column displays the grace period of licenses and its expiry date.

You can use **Filter by attribute** to view required information.

Click **Refresh** icon to refresh the table.

Event Analytics

Event Analytics includes the following topics:

- Alarms
- Events
- Accounting

Viewing Backup

You can view the following information on Backup tab.

- **Switch** column displays the switch name.
- **Backup Date** column displays the backup date.
- **Backup Tag** column displays the backup tag name.
- **Backup Type** column displays the type of backup.
- **Configuration File** column displays the configuration files that are archived for that device.

You can use **Filter by attribute** to view required information.

Click **Refresh** icon to refresh the table.

The following table describes the actions you can perform in this tab:

Action	Description
Copy to bootflash	Refer to Copy Bootflash, on page 12.
Compare	Refer to Compare Configuration Files.
Export	Refer to Export Configuration.
Edit tag	To edit a tag of a switch. Choose check box for a required switch, choose **Actions** > **Edit tag** and click **OK**.
Mark as golden	To mark switch as a golden backup. Choose check box for a required switch, choose **Actions** > **Mark as golden**. A confirmation window appears, click **Confirm**. Refer to Golden backup section for more information.
Remove as golden	To remove switch from a golden backup. Choose check box for a required switch, choose **Actions** > **Remove as golden**. A confirmation window appears, click **Confirm**.
Delete	To delete switch from a backup. Choose check box for a required switch, choose **Actions** > **Delete**. A confirmation window appears, click **Confirm**.

This sections contains the following:

Copy Bootflash

You can copy the configuration files to the same device, to another device, or multiple devices concurrently.

Perform the following task to view the status of tasks:

Procedure

Step 1 From SAN Controller home page, choose **SAN> Switch > Switch Overview > Backup**.

Step 2 Click **Copy to bootflash**.

Copy to bootflash page appears, displaying the **Source Configuration Preview** and **Selected Devices** area.

Source Preview area shows the contents of running/startup/version configuration file which is copied to the devices.

Step 3 In the **Selected Devices** area, check the device name check box to copy the configuration to the device.

Note You can select multiple destination devices to copy the configuration.

The selected devices area shows the following fields:

- Device Name - Specifies the target device name to which the source configuration is copied.
- IP Address - Specifies the IP Address of the destination device.
- Group - Specifies the group to which the device belongs.
- Status - Specifies the status of the device.

Step 4 Click **Copy**.

A confirmation window appears.

Step 5 Click **Yes** to copy the configuration to the destination device configuration.

Compare Configuration Files

This feature allows you to compare the configuration file with another version of the same device or with the configuration file of another device.

Perform the following task to compare the configuration files.

Procedure

Step 1 Check the check box and select two configuration files to compare.

The first file that you selected is designated as Source and the second configuration file is designated as the Target file.

Step 2 Navigate to **SAN> Switch > Switch Overview > Compare**.

Step 3 Click **Compare Configuration**.

View Config Diff page appears, displaying the difference between the two configuration files.

The Source and Target configuration files content is displayed in two columns. From the drop-down list in the right-top corner, choose **All** to view the entire configuration. You can also choose **Changed** to view the configuration differences of the configuration files.

The differences in the configuration file are show in the table, with legends.

- **Red**: Diff configuration details.
- **Green**: New added configuration.
- **Blue**: Modified configuration details.

Step 4 Click **Copy to Target** to copy the source configuration to the target configuration file. Click **Cancel** to revert to the configuration details page.

The Copy Configuration window displays the source configuration preview and the target device of the destination configuration. The selected devices area shows the following fields:

- Device Name—Specifies the target device name to which the source configuration is copied.
- IP Address—Specifies the IP Address of the destination device.
- Group—Specifies the group to which the device belongs.
- Golden Config—Specifies the version of the destination configuration.
- Status—Specifies the status of the device.

Step 5 Click **Yes** to copy the configuration to the destination device configuration.

Export Configuration

You can export a configuration file from the SAN Controller server. Perform the following task to export a configuration file.

Procedure

Step 1 From SAN Controller home page, choose **Configure > Backup**, select a configuration to export.

Step 2 Click **Export Configuration**.

The files are downloaded in your local system. You can use the third-party file transfer tools to transfer these files to an external server.

Viewing of Port Usage

You can view the following information on Port Usage tab.

- **Port Speed** column displays the speed of the port.
- **Used Ports** column displays the total ports with the mentioned port speed.
- **Available Ports** column displays the available ports for the port speed.
- **Total Ports** column displays the total ports with the mentioned speed.
- **Estimated Day Left** column displays the estimated days left for the ports.

You can use **Filter by attribute** to view required information.

Click **Refresh** icon to refresh the table.

Used ports displays the total used ports for the selected switch.**Total ports** displays the total available ports for the selected switch.

Viewing Bootflash

You can view the following information on Bootflash tab.

- **Primary Bootflash Summary** card displays the total, used and available space.
- **Secondary Bootflash Summary** card displays the total, used and available space.
- **Directory Listing** area displays check box for **Primary Bootflash** and **Secondary Bootflash**.

  This area shows the filename, size, and last modified date for all the files and directories on the switch bootflash. Choose **Actions** > **Delete** to delete files to increase the available space on the switch.

Device Manager

See Device Manager chapter for descriptions and instructions for using the Cisco MDS 9000 Device Manager.

Note Device Manger session is terminated when you navigate to another tab on the **Switch Overview** screen.

Blades

You can view the interfaces of the UCS switches through **SAN** > **Switches** > **Switch Overview**, on the SAN Controller Web UI.

Note Ensure that the UCS switches are listed on SAN Controller and the status of these switches are correct. You can view these tabs only for UCS switches.

Blades tab displays information of all server blades attached to the UCS FI.

The UCS has three tabs namely:

- Blades
- vNICs
- vHBAs

The blades tab displays all blade information as cards. Click **More Details** icon on each blade area to view details on the side panel of the selected blade.

You can click **Collapse All** or **Expand All** icon to collapse all or expand all blade areas respectively.

Blades tab displays information of all server blades attached to the UCS FI. Primary UCS FI only in redundancy setup or standalone UCS FI are displayed.

vNICs

vNICs tab displays the list of vNIC for that UCS FI. Click the chart icon will show the 24 hour traffic for the vNIC.

vHBAs

vHBAs tab displays the list of vHBA for that particular UCS FI. Click the chart icon to view 24hour traffic for the vHBA.