Cisco DCNM User Roles

Cisco DCNM User Roles

Cisco DCNM defines what operations a user can perform in Cisco DCNM Web Client by controlling what features are available in the menu and tool bar items. Cisco DCNM role-based authorization limits access to the server operations depending on the user roles.

Cisco DCNM has two sets of credentials, namely:

- Device credentials—used to discover and manage devices.
- Cisco DCNM credentials—used to access the Cisco DCNM server.

This document describes about DCNM credentials and how user roles are mapped to specific set of DCNM server operations.

This chapter contains following sections:

Cisco DCNM Users

Cisco DCNM user-based access allows the administrator to control the access to the Cisco DCNM server by using the DCNM client (Web Client or LAN client). The user access is secured by a password.

Note Beginning from Release 10.0(x), DCNM doesn't allow you to reset the password using adduser script. Log on to Cisco DCNM Web UI to reset the password. Use the adduser script to add a new DCNM user on the existing DCNM setup.

DCNM Roles

Cisco DCNM performs authorization of access to the users based on roles. The role-based authorization limits access to the Cisco DCNM server operations based on the roles to which the users are assigned. Cisco DCNM doesn't define new roles to access the DCNM server; however, the Cisco DCNM leverages the existing roles that are supported on the devices monitored, such as Cisco MDS 9000 Series Switches, and Cisco Nexus Switches.

The table below lists the roles supported by Cisco DCNM:

Role	Description
global-admin	Introduced in Cisco Nexus 5000 series switches and FCoE, a role to administrate LAN and SAN features.
network-admin	General role to administrate LAN features.
lan-network-admin	General role to administrate LAN features.
san-network-admin	General role to administrate SAN features.
san-admin	Introduced in Cisco Nexus 5000 series switches and FCoE, a role to administrate SAN features.
server-admin	Introduced in the FlexAttach feature, a role that administrates FC server host feature.
sme-admin	Introduced in the Storage Media Encryption (SME) feature, a role that administrates SME feature.
sme-stg-admin	Introduced in the Storage Media Encryption (SME)) feature, a role that administrates SME storage.
sme-kmc-admin	Introduced in the Storage Media Encryption (SME) feature, a role that administrates SME Key Management.
sme-recovery	Introduced in the Storage Media Encryption (SME) feature, a role that administrates SME recovery.
network-operator	General network operator role.
device-upg-admin	This role is added to perform operations only in Image Management window.
access-admin	This role is introduced to perform operations in Interface Manager window for all fabrics.

In a typical enterprise environment, users and their roles are defined in a centralized place such as, TACACS+, RADIUS, or LDAP. As Cisco DCNM supports the existing device roles, the administrator need not define new roles specifically.

User Role Assignment by RADIUS and TACACS+

Cisco DCNM supports the assignment of a user role by the RADIUS or TACACS+ server that grants a user access to the Cisco DCNM client. The user role assigned to a user is in effect for the current session in the Cisco DCNM client only.

To assign a Cisco DCNM user role by RADIUS, configure the RADIUS server to return the RADIUS vendor-specific attribute 26/9/1, which is the Cisco-AV-Pair attribute. To assign a Cisco DCNM user role by TACACS+, the TACACS+ server must return a cisco-av-pair attribute-value pair. If an authentication response doesn't assign the user role, Cisco DCNM assigns the User role. Table 1: Cisco DCNM User Role Assignment Values , on page 3 shows the supported attribute-value pair values for each Cisco DCNM user role.

Table 1: Cisco DCNM User Role Assignment Values

Cisco DCNM Role	RADIUS Cisco-AV-Pair Value	TACACS+ Shell cisco-av-pair Value
User	`shell:roles = "network-operator"`	`cisco-av-pair=shell:roles="network-operator"`
Administrator	`shell:roles = "network-admin"`	`cisco-av-pair=shell:roles="network-admin"`

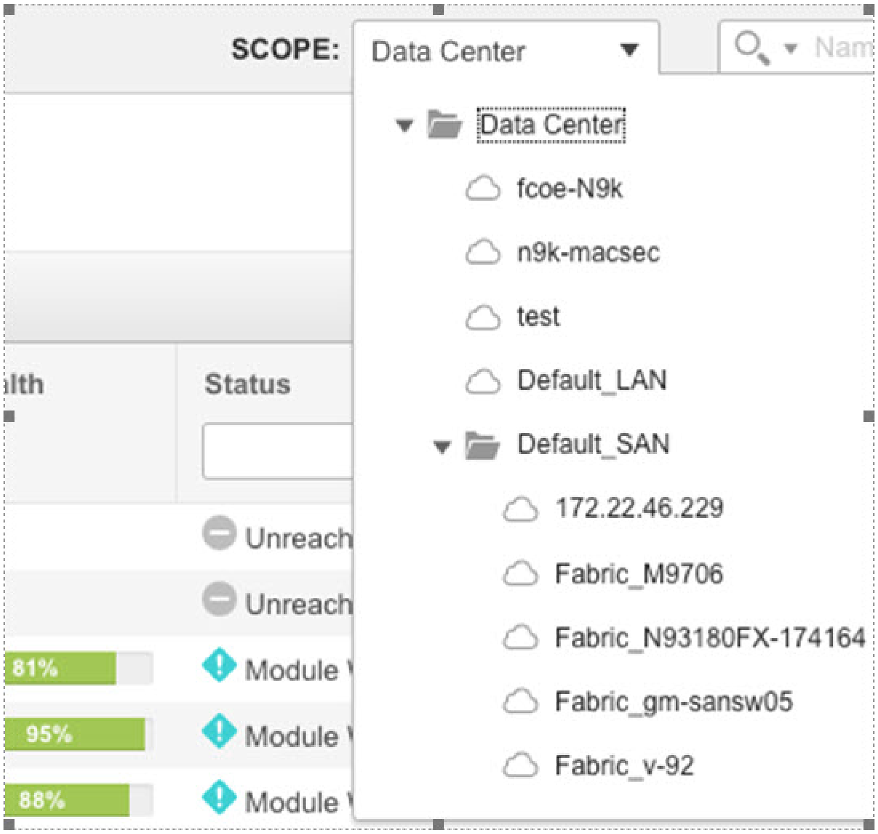
DCNM-Scope Mapping

Cisco DCNM allows you to add fabric names in TACACS using cisco-av-pairs. You can enable different AV pairs for any supported attribute value.

Cisco-av-pair=shell:roles="network-admin": **dcnm-access**="n9k-macsec fcoe-N9k"

Cisco-av-pair=shell:roles="network-admin": **dcnm-access**="fabric_M9706 Fabric_v-92"

These av-pairs appear on the Cisco DCNM **Web UI** > **Scope** drop-down list, based on the user access.



Roles from Cisco DCNM Perspective

Cisco DCNM perspective defines the operations that you can perform on the Cisco DCNM client by controlling the menu and tool bar items. Different perspectives define different set of operations.

For example, the **Admin** perspective allows all the operations by showing all the menu and tool bar items whereas **Operator** perspective allows limited set of operation by hiding Admin and Config Menu items.

Each DCNM user role is mapped to a particular DCNM perspective, which allows limited access to server features. DCNM clients support following four perspectives:

Table 2: DCNM Roles and Perspectives Mapping Table, on page 4 describes how DCNM roles are mapped to client perspectives.

Table 2: DCNM Roles and Perspectives Mapping Table

Role	Perspective
global-admin	Admin Perspective
network-admin	
san-admin	
san-network-admin	
lan-network-admin (Web Client)	
server-admin	Server Admin Perspective
sme-admin	SME Perspective
sme-sgt-admin	
sme-kmc-admin	
sme-recovery	
network-operator	Operator Perspective
lan-network-admin (SAN Client)	
access-admin	
device-upg-admin	

Admin Perspective

Admin Perspective can be accessed through the Cisco DCNM Web Client and SAN Client only, by the users who are assigned the role of global-admin, network-admin, san-admin, san-network-admin, and lan-network-admin.

Web Client Admin Perspective

Web client admin perspective has full control of the DCNM server and can access all the features. Via the access to the Admin menu items, the users also have full control of Cisco DCNM authentication settings.

SAN Client Admin Perspective

SAN client admin perspective has full control of the DCNM server and can access all the features. All the top-level menu items are accessible.

Server Admin Perspective

Server admin perspective can be accessed via web client and SAN client only by the users who are assigned the role of server-admin.

Web Client Server Admin Perspective

Web client server admin perspective has access to all the web client features. Via the access to the Admin menu items, the users also have full control of Cisco DCNM authentication settings.

SME Perspective

Storage Media Encryption (SME) perspective is designed for sme-admin, sme-sgt-admin, sme-kmc-admin, and sme-recovery role-based users. It is categorized to five different sme admin perspective according to the roles:

Web Client SME Admin Perspective

Web client sme admin perspective is designed to sme-admin role users who have no access to Admin and Config menu items in the Web client and can’t use features under those menu items. On the other hand, the SME provision features are accessible.

SME Storage Perspective

SME storage perspective is designed to the sme-stg-admin role users. sme-stg-admin role users have same perspective as sme-admin role except you can’t manage the key management features.

SME Key Management Perspective

SME key management perspective is designed to the sme-kmc-admin role users. sme-kmc-admin role users have same perspective as sme-admin role except that you can’t perform SME configurations.

SME Recovery Perspective

SME recovery perspective is designed to the sme-recovery role users for master key recovery. sme-recovery role users have same perspective as sme-admin role except that you can’t perform the storage and key management features.

SAN Client SME Perspective

SAN client SME perspective has no access to Discover button, Fabrics, and License Files tabs. All the SME-related perspective would not be able to manage Fabric Manager users or connected clients, and operator perspective.

Operator Perspective

Operator perspective is designed for device-upg-admin, access-admin, network-operator and lan-network-admin role users, and lan-network-admin role only has SAN client operator perspective.

Web Client Operator Perspective

Web client operator perspective has no access to Admin and Config menu items and the features under those menu items can’t be used. All the other features can be used.

SAN Client Operator Perspective

SAN client operator perspective has no access to Discover button, Fabrics and License Files tabs, and wouldn’t be able to manage Fabric Manager users or connected clients.

User Access for Cisco DCNM

From Release 11.3(1), Cisco DCNM offers the user access based on your network security requirements. The following user roles allow access to DCNM via SSH or console that is introduced with Release 11.3(1).

- **sysadmin user**

  This DCNM OS user role is considered as the system administrator.

  sysadmin user role allows you to run **appmgr** and other system commands for managing and debugging the system such as **reboot**, **tcpdump**, etc. However, the user can function as a **root** user by using the **su** command.

  Note The **root** user role is required to read log files.

- **SSH access by user root**

  On a Native HA setup using DCNM Management IPv4 VIP, SSH access with **root** user is allowed from DCNM to DCNM Computes. SSH access with **root** user is always allowed between HA peers. When adding a second node to a Standalone system or to a Native-HA setup (while restoring the secondary node), SSH access must be permitted for the installation to complete successfully.

  By default, SSH access with **root** user is disabled. Alternatively, you can use the **sysadmin** user.

  You can change the SSH access with **root** user by using the following command:

  appmgr root-access {permit|deny|without-password}

Note The DCNM GUI root user is no longer created. Alternatively, use the Admin user role to log on to the DCNM Web UI.