

CISCO 12.1.3 Enhanced Role-Based Access Control User Guide

[Home](#) » [Cisco](#) » CISCO 12.1.3 Enhanced Role-Based Access Control User Guide 



Contents

1

New and Changed Information

2

Enhanced Role-based Access Control

3

Enhanced RBAC Use-Cases

4

Copyright

5

Documents / Resources

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
NDFC release 12.1.3	Reorganized content	Content within this document was originally provided in the Cisco NDFC-Fabric Controller Configuration Guide or the Cisco NDFC-SAN Controller Configuration Guide. Beginning with release 12.1.3, this content is now provided solely in this document and is no longer provided in those documents.

Enhanced Role-based Access Control

Starting from Cisco Nexus Dashboard Fabric 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 Change Approver
- NDFC Change Deployer
- 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
NDFC Change Approver	Read/Write
NDFC Change Deployer	Read/Write
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:

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

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

NDFC Access Admin

A user with the NDFC Access Admin role can perform operations only in the 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 Cisco Nexus Dashboard Fabric Controller access admin role cannot perform the following actions:

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

 The icons and buttons are grayed out for this role when the fabric or Cisco Nexus Dashboard Fabric Controller is in deployment-freeze mode.

NDFC Change Approver

The NDFC Change Approver role became available as part of the change control and rollback features, introduced in NDFC release 12.1.3. See [Change Control and Rollback](#) for more information.

Users with the NDFC Change Approver privilege can approve change control tickets.

A user that is assigned with the NDFC Change Approver role can double-check changes that are associated with a specific ticket and approve or deny those changes.

NDFC Change Deployer

The NDFC Change Deployer role became available as part of the change control and rollback features, introduced in NDFC release 12.1.3. See [Change Control and Rollback](#) for more information.

Users with the NDFC Change Deployer privilege can deploy change control tickets.

Once a change control ticket is approved by a user with the NDFC Change Approver role, that ticket is then available to any user that is assigned with the NDFC Change Deployer role, who can then deploy the changes that have moved to the deployment stage in the change control workflow.

NDFC Device Upgrade Admin

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

See [Image Management: LAN](#) for more information.

NDFC Network Admin

A user with the NDFC Network Admin role can perform all the operations in Cisco Nexus Dashboard Fabric Controller.

From Cisco Nexus Dashboard Fabric Controller Release 12.1.1e, a user with this role can perform all operations for MSD fabrics in Networks and VRFs.


You can freeze a particular fabric or all fabrics in Cisco Nexus Dashboard Fabric Controller if you are a user with the NDFC Network Admin role.

NDFC Network Admin

A user with the NDFC Network Admin role can perform all the operations in Cisco Nexus Dashboard Fabric Controller.

From Cisco Nexus Dashboard Fabric Controller Release 12.1.1e, a user with this role can perform all operations for MSD fabrics in Networks and VRFs.

You can freeze a particular fabric or all fabrics in Cisco Nexus Dashboard Fabric Controller if you are a user with the NDFC Network Admin role.

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

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.

NDFC Network Stager

A user with the NDFC Network Stager role can make configuration changes on Cisco Nexus Dashboard Fabric 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 Cisco Nexus Dashboard Fabric 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.

Choosing Default Authentication Domain

By default, the 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, see <https://www.cisco.com/c/en/us/td/docs/dcn/nd/2x/user-guide/cisco-nexus-dashboarduser-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
<ul style="list-style-type: none"> User has a single role. All APIs and resources are accessed with this single role. 	<ul style="list-style-type: none"> User can have a different role in different Nexus Dashboard for security domains. Security domain contains single Nexus Dashboard, and each Nexus 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 and restricted access are grayed out based on security domain associated with 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, networkstager, access-admin are in NDFC. Support for legacy roles for backward compatibility. Nexus Dashboard 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-avpair=shell:roles="networkoperator" dcnm-access="group1 group2 group5"
Network-Admin	shell:roles = "network-admin" dcnm-access="group1group2 group5"	cisco-avpair=shell:roles="networkadmin" 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>

Enhanced RBAC Use-Cases

There are various fabrics in NDFC. By default a user is an admin for all the fabrics. For an example, a username Cisco can have admin role access to a Fabric-A and stager role access to another FabricB. On Nexus Dashboard, all security policies are part of security domains. You can create the user and give access to these security domains.

To create a user and define specific roles, perform the following steps:

1. To create user in security domains:

- a. Log in to Nexus Dashboard with admin role and navigate to Administrative tab.
- b. On Security Domain tab, click Create Security Domain and create the following security domains:
 - all – Similar to network-admin role. This domain has administrative access to Nexus Dashboard and NDFC service application.
 - cisco-admin – full network-admin access to Fabric-A
 - cisco-stager – network-stager only access to Fabric-B

2. To create a local user Cisco.

- a. Navigate to Users > Local.
- b. On Local tab, click Create Local User.
The Create Local User window appears.
- c. Enter Cisco in User ID text field, provide appropriate passwords in respective fields.
- d. After you create a Cisco user, navigate to Local window, click on ellipses icon in Cisco username row and then click Edit User.

The Edit User window appears.


3. On Edit User window, by default, all security domain exists. Click Add Security Domain and Roles to add other security domains.

The Add Security Domain and Roles window appears.

- a. Choose cisco-admin domain from option drop-down list and choose NDFC Access Admin check box and then click Save.
- b. Repeat step a to add cisco-stager domain for NDFC Network Stager role.
- c. To associate security domains to respective fabric sites, do the following:
On Nexus Dashboard, navigate to Sites window. Click on Fabric-A site name.
A slide-in pane appears. You can view all security domain for the Fabric-A site.
- d. To add the Cisco user as network-admin for Fabric-A, click Ellipse icon and Edit Site.
- e. Delete all security domain and add network-admin domain and save the changes.


Similarly you can add for network-stager domain.

- f. Log out from Nexus Dashboard and log in back as Cisco user.

 The user role Cisco can view only NDFC related options on Nexus Dashboard based on the permissions. The user access restricted to Nexus Dashboard services.

- g. Navigate to NDFC application.

The user Cisco can perform operations on two sites on NDFC, as the user is assigned as network-admin role for Fabric-A and network-stager role for Fabric-B.

 Network-admin role can create an interface for Fabric-A and deploy it. Whereas network-stager role can create an interface for Fabric-B, but access is restricted to deploy.

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: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2017-2023 Cisco Systems, Inc. All rights reserved.

Documents / Resources

 <small>Configuring Enhanced Role-Based Access Control, Release 12.1.3</small>	CISCO 12.1.3 Enhanced Role-Based Access Control [pdf] User Guide 12.1.3, 12.1.3 Enhanced Role-Based Access Control, Enhanced Role-Based Access Control, Role-Based Access Control, Access Control
--	--