Role Based Access Control

Table 1: Feature History

Feature Name	Release Information	Feature Description
Co-Management: Granular Role-Based Access Control	Cisco Catalyst SD-WAN Manager Release 20.13.1	This feature introduces role-based access control (RBAC) based on sites, scope, or roles. It is a method of authorizing system access for users based on a combination of role and scope of a user. You can create scope, users and roles with required read and write permissions for Cisco SD-WAN Manager policies. RBAC prevents unauthorized access and reduces the risk of data breaches and other security incidents.
Canadian French Language Support on Cisco Catalyst SD-WAN Manager	Cisco Catalyst SD-WAN Manager Release 20.13.1	Added support for using Canadian French for the Cisco Catalyst SD-WAN Manager user interface.

Information About RBAC

Information About Role Based Access Control

Role-Based Access Control (RBAC) is a method of restricting or authorizing system access for users based on user roles and scope. A role defines the privileges of a user in the system and the locale defines the

organizations (domains) that a user is allowed access. Because users are not directly assigned privileges, management of individual user privileges is simply a matter of assigning the appropriate roles and scopes. A user is granted write access to desired system resources only if the assigned role grants the access privileges and the assigned locale allows access.

User: is the entity that performs different actions in Cisco SD-WAN Manager. A user belongs to a role.

Roles: define the permissions (Read, Write or Deny) allowed for a user for different APIs or functionalities.

Scope: define the set of objects (sites, devices or templates) on which a user can perform actions.

When **Read** or **Write** is selected, the user can view and make changes for the selected features. When **Read** is selected, the user can only view information. When **Deny** is selected, the user can neither view or make changes to the Cisco IOS XE Catalyst SD-WAN.

System default roles cannot be changed or modified. The Cisco IOS XE Catalyst SD-WAN software provides the following system default roles:

- **basic**: The basic role is a system default role and is pre-built-in Cisco SD-WAN Manager. You cannot modify or delete. If you want to modify the role, you must make a copy of it and then modify it as a new customer role.
- **operator**: The operator role is also a configurable role and can be used for any users and privilege levels. This role is designed to include users who have permission only to view information.
- **netadmin**: The netadmin role is a non-configurable role. By default, this role includes the **admin** user. You can add other users to this role. Users with this role are permitted to perform all operations on the device.
- **network_operations**: The **network_operations** role is a non-configurable role. Users in this role can perform all non-security-policy operations on the device and only view security policy information. For example, users can create or modify template configurations, manage disaster recovery, and create non-security policies such as an application aware routing policy or Cflowd policy.
- **security_operations**: The **security_operations** role is a non-configurable role. Users in this role can perform all security operations on the device and only view non-security-policy information. For example, users can manage umbrella keys, licensing, IPS signatures auto update, TLS/SSL proxy settings, and so on.

Users of the **network_operations** role are authorized to apply policies to a device, revoke applied policies, and edit device templates. Users of the **security_operations** role require **network_operations** users to intervene on day-0 to deploy a security policy on a device and on day-N to remove a deployed security policy. However, after a security policy is deployed on a device, **security_operations** users can modify the security policy without needing the **network_operations** users to intervene.

Note Only netadmin users can view the running and local configuration. Users associated with a predefined operator role do not have access to the running and local configurations. The predefined role operator has only read access for the template configuration. If you need only a subset of admin user privileges, then you need to create a new role with the selected features from the features list with both read and write access and associate the role with the custom user.

Privileges for Role-Based Access

Role-based access privileges are arranged into five categories, which are called *tasks:*

- Interface—Privileges for controlling the interfaces on the Cisco IOS XE Catalyst SD-WAN device.
- Policy—Privileges for controlling the control plane policy, OMP, and data plane policy.
- Routing—Privileges for controlling the routing protocols, including BFD, BGP, OMP, and OSPF.
- Security—Privileges for controlling the security of the device, including installing software and certificates. Only users belonging to the **netadmin** group can install software on the system.
- System—General system-wide privileges.

Role-Based Access Control by VPN

Role-based access control (RBAC) is the process of restricting user access to network configurations and resources. In RBAC, users are assigned roles depending on the resources they need access to. The RBAC by VPN feature helps you to manage and control access to your network based on the VPNs. It involves setting permissions and privileges to enable access to authorized users.

RBAC by VPN

Role-based access by VPN allows a network administrator to define VPN groups with one or more network segments. The network administrator can associate a user with a VPN group that restricts user access to devices in the network and features of Cisco SD-WAN Manager.

RBAC by VPN provides the following restricted access to users configured with a VPN group:

- Access to VPN Dashboard
- Monitor devices, network, and application status via VPN dashboard
- VPN dashboard information restricted to devices with segments in the VPN group
- Monitor option restricted to devices with segments in the VPN group
- Interface monitoring on each device restricted to interfaces of segments in the VPN group

VPN Dashboard Overview

Users configured with VPN group can access only the VPN Dashboard, and it is read-only access. User with Admin access can create the VPN groups and has access to both Admin Dashboard and VPN Dashboard(s). Admin user can access these dashboards by choosing **Dashboard** from the Cisco SD-WAN Manager menu.

Role-Based Access with AAA

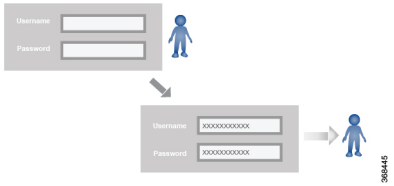
The Cisco Catalyst SD-WAN AAA software implements role-based access to control the authorization permissions for users on Cisco IOS XE Catalyst SD-WAN devices. Role-based access consists of three components:

- Users are those who are allowed to log in to a Cisco IOS XE Catalyst SD-WAN device.
- User groups are collections of users.

- Privileges are associated with each group. They define the commands that the group's users are authorized to issue.

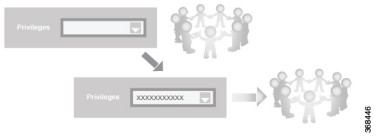
Users and User Groups

All users who are permitted to perform operations on a Cisco IOS XE Catalyst SD-WAN device must have a login account. For the login account, you configure a username and a password on the device itself. These allow the user to log in to that device. A username and password must be configured on each device that a user is allowed to access.

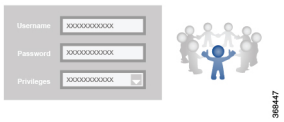


The Cisco Catalyst SD-WAN software provides one standard username, **admin**, which is a user who has full administrative privileges, similar to a UNIX superuser. By default, the **admin** username password is **admin**. You cannot delete or modify this username, but you can and should change the default password.

User groups pool together users who have common roles, or privileges, on the Cisco IOS XE Catalyst SD-WAN device. As part of configuring the login account information, you specify which user group or groups that user is a member of. You do not need to specify a group for the **admin** user, because this user is automatically in the user group **netadmin** and is permitted to perform all operations on the Cisco IOS XE Catalyst SD-WAN device.



The user group itself is where you configure the privileges associated with that group. These privileges correspond to the specific commands that the user is permitted to execute, effectively defining the role-based access to the Cisco Catalyst SD-WAN software elements.



The Cisco Catalyst SD-WAN software provides the following standard user groups:

- **basic**: The basic group is a configurable group and can be used for any users and privilege levels. This group is designed to include users who have permission to both view and modify information on the device.
- **operator**: The operator group is also a configurable group and can be used for any users and privilege levels. This group is designed to include users who have permission only to view information.
- **netadmin**: The netadmin group is a non-configurable group. By default, this group includes the **admin** user. You can add other users to this group. Users in this group are permitted to perform all operations on the device.
- Minimum supported release: Cisco vManage Release 20.9.1

network_operations: The **network_operations** group is a non-configurable group. Users in this group can perform all non-security-policy operations on the device and only view security policy information. For example, users can create or modify template configurations, manage disaster recovery, and create non-security policies such as application aware routing policy or CFlowD policy.

- Minimum supported release: Cisco vManage Release 20.9.1

  security_operations: The **security_operations** group is a non-configurable group. Users in this group can perform all security operations on the device and only view non-security-policy information. For example, users can manage umbrella keys, licensing, IPS signatures auto update, TLS/SSL proxy settings, and so on.

Users of the **network_operations** group are authorized to apply policies to a device, revoke applied policies, and edit device templates. Users of the **security_operations** group require **network_operations** users to intervene on day-0 to deploy security policy on a device and on day-N to remove a deployed security policy. However, after a security policy is deployed on a device, **security_operations** users can modify the security policy without needing the **network_operations** users to intervene.

Note Only admin users can view running and local configuration. Users associated with predefined operator user group do not have access to the running and local configurations. The predefined user group operator has only read access for the template configuration. If you need only a subset of admin user privileges, then you need to create a new user group with the selected features from the features list with both read and write access and associate the group with the custom user.

Privileges for Role-Based Access

Role-based access privileges are arranged into five categories, which are called *tasks:*

- Interface—Privileges for controlling the interfaces on the Cisco IOS XE Catalyst SD-WAN device.
- Policy—Privileges for controlling control plane policy, OMP, and data plane policy.
- Routing—Privileges for controlling the routing protocols, including BFD, BGP, OMP, and OSPF.
- Security—Privileges for controlling the security of the device, including installing software and certificates. Only users belonging to the **netadmin** group can install software on the system.
- System—General systemwide privileges.

The tables in the following sections detail the AAA authorization rules for users and user groups. These authorization rules apply to commands issued from the CLI and to those issued from Netconf.

User Authorization Rules for Operational Commands

The user authorization rules for operational commands are based simply on the username. Any user who is allowed to log in to the Cisco IOS XE Catalyst SD-WAN device can execute most operational commands. However, only the **admin** user can issue commands that affect the fundamental operation of the device, such as installing and upgrading the software and shutting down the device.

Note that any user can issue the **config** command to enter configuration mode, and once in configuration mode, they are allowed to issue any general configuration command. Also, any user is allowed to configure their password by issuing the **system aaa user** *self* **password** *password* command and then committing that

configuration change. For the actual commands that configure device operation, authorization is defined according to user group membership. See User Group Authorization Rules for Configuration Commands.

The following tables lists the AAA authorization rules for general CLI commands. All the commands are operational commands except as noted. Also, some commands available to the "admin" user are available only if that user is in the "netadmin" user group.

CLI Command	Any User	Admin User
clear history	X	X
commit confirm	X	X
complete-on-space	X	X
config	X	X
exit	X	X
file	X	X
help	X	X
[no] history	X	X
idle-timeout	X	X
job	X	X
logout	—	X (users in netadmin group only)
monitor	X	X
nslookup	X	X
paginate	X	X
ping	X (users in netadmin group only)	X (users in netadmin group only)
poweroff	—	X(users in netadmin group only)
prompt1	X	X
prompt2	X	X
quit	X	X
reboot	—	X (users in netadmin group only)
request aaa request admin-tech request firmware request interface-reset request nms request reset request software	—	X (users in netadmin group only)
request execute request download request upload	X	X

CLI Command	Any User	Admin User
request (everything else)	—	X
rollback (configuration mode command)	—	X (users in netadmin group only)
screen-length	X	X
screen-width	X	X
show cli	X	X
show configuration commit list	X	X
show history	X	X
show jobs	X	X
show parser dump	X	X
show running-config	X	X
show users	X	X
system aaa user *self* password *password* (configuration mode command) (Note: A user cannot delete themselves)		
tcpdump	X	X
timestamp	X	X
tools ip-route	X	X
tools netstat	X	X
tools nping	X	X
traceroute	X	X
vshell	X (The availability of vshell command is unavailable to all users that are not in netadmin group in Cisco vManage Release 20.9.5.)	X (The vshell AAA authorized access is limited only to users that are in netadmin group.)

User Group Authorization Rules for Operational Commands

The following table lists the user group authorization roles for operational commands.

Operational Command	Interface	Policy	Routing	Security	System
clear app		X			
clear app-route		X			
clear arp	X				
clear bfd			X		X
clear bgp			X		X
clear bridge	X				
clear cellular	X				
clear control				X	
clear crash					X
clear dhcp					X
clear dns					X
clear igmp			X		
clear installed-certificates				X	
clear interface	X				
clear ip			X		
clear notification					X
clear omp			X		
clear orchestrator				X	
clear ospf			X		
clear pim			X		
clear policy		X			
clear pppoe	X				
clear system					X
clear tunnel				X	
clear wlan	X				
clear ztp				X	X
clock					X

Operational Command	Interface	Policy	Routing	Security	System
debug bgp			X		
debug cellular	X				
debug cflowd		X			
debug chmgr					X
debug config-mgr					X
debug dhcp-client					X
debug dhcp-helper					X
debug dhcp-server					X
debug fpm		X			
debug ftm					X
debug igmp			X		
debug netconf					X
debug omp			X		
debug ospf			X		
debug pim			X		
debug resolver			X		
debug snmp					X
debug sysmgr					X
debug transport					X
debug ttm					X
debug vdaemon				X	X
debug vrrp				X	
debug wlan	X				
request certificate				X	
request control-tunnel				X	
request controller				X	
request controller-upload				X	

Operational Command	Interface	Policy	Routing	Security	System
request csr				X	
request device				X	
request device-upload				X	
request on-vbond-controller				X	
request port-hop				X	
request root-cert-chain				X	
request security				X	
request vedge				X	
request vedge-upload				X	
request vsmart-upload				X	
show aaa					X
show app		X			
show app-route		X			
show arp	X				
show bfd			X		X
show bgp			X		
show boot-partition					X
show bridge	X				
show cellular	X				
show certificate				X	
show clock					X
show control				X	X
show crash					X
show debugs—same as debug commands					
show dhcp					X
show external-nat				X	X
show hardware					X

Operational Command	Interface	Policy	Routing	Security	System
show igmp			X		
show interface	X				
show ip			X		X
show ipsec				X	
show licenses					X
show logging					X
show multicast			X		
show nms-server					X
show notification					X
show ntp					X
show omp		X	X		X
show orchestrator				X	
show ospf			X		
show pim			X		
show policer		X			
show policy		X			
show ppp	X				
show pppoe	X				
show reboot					X
show security-info				X	
show software					X
show system					X
show transport					X
show tunnel				X	
show uptime					X
show users					X
show version					X
show vrrp	X				

Operational Command	Interface	Policy	Routing	Security	System
show wlan	X				
show ztp				X	

User Group Authorization Rules for Configuration Commands

The following table lists the user group authorization rules for configuration commands.

Configuration Command	Interface	Policy	Routing	Security	System
apply-policy		X			
banner					X
bfd			X		X
bridge	X				
omp		X	X		X
policy		X			
security				X	X
snmp					X
system					X
vpn interface	X				
vpn ip			X		
vpn router			X		
vpn service			X		
vpn (everything else, including creating, deleting, and naming)					X
wlan	X				

RBAC By Resource Group Overview

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.5.1a and Cisco vManage Release 20.5.1

RBAC by resource groups is a method of restricting or authorizing system access for users based on user groups and resource groups. A user group defines the privileges of a user in the system and the resource group defines the organizations (domains) to which a user is allowed access. Because users are not directly assigned privileges, management of individual user privileges is simply a matter of assigning the appropriate user and resource groups.

For large Cisco Catalyst SD-WAN deployments across multiple geographical locations, you can split the network administration among different regional adminstrators.

Based on the user groups and resources groups to which network administrators are assigned, we can broadly classify them as Global Administrators and Regional Administrators. Global administrators have access to resources in every resource group and have full read-write privileges for all the features. Regional Administrators group have full read-write privileges for all the features, but the resources they can access is controlled by the resource groups to which they are assigned.

Global Admin

User accounts in the global resource group have access to all resources. A global admin is responsible for overseeing the entire network, but not involved in the operations of the individual devices on a daily basis. The global admin can assign devices to their corresponding regions, assign the regional admin accounts, manage the controllers, maintain sharable and centralized configurations, and when necessary, operate on the individual devices.

Any user in a single tenant setup with netadmin privileges and also part of global resource group is considered as global admin. Default admin user on Cisco SD-WAN Manager is also a global-admin, and that user can assign more global-admins. Global resource group encompasses all the WAN edges, controllers in the single view.

Global admin can switch to view only a specific resource group and can create templates. Local resource group admins, also called regional admins can clone the global templates and reuse them within their resource groups.

Regional Admin

The regional admins are responsible for day-to-day operations (configuration, monitoring, onboarding, and so on) for devices in their corresponding regions. They should not have access to or visibility into devices outside of their region. The following user groups can be created:

- resource group admin – full read/write access to devices in the corresponding resource group, can troubleshoot, monitor, attach or detach templates for the WAN edges in their group
- resource group operator – read-only access to WAN edges within their resource group
- resource group basic – basic access

Resource group admins can create new templates and attach or detach to the WAN edges in their group. They can also copy global templates and re-use them.

Resource group decides which resources the user has access to. However, the level of access is controlled by the existing user group.

- If user is in **resource_group_a** and user group **resource_group_admin**, they have full read/write access to all resources in resource_group_a.
- If user is in **resource_group_a** and user group **resource_group_operator**, they have read only access to all resources in **resource_group_a**.
- If user is in **resource_group_a** and user group **resource_group_basic**, they have read only access to interface and system resources in **resource_group_a**.

Global Resource Group

Global group is a special system pre-defined resource group that has different access control rules.

- Users within this group are considered as global-admins, who can have full access to all resources (devices, templates and policies) in the system and they can manage the resource groups and assign resources and users to groups.
- All other users have read-only access to resources within this group.
- The system default admin account (or tenantadmin account in a multi-tenant setup) is always in this group. This privilege cannot be changed. However, the admin account may add/remove other user accounts to or from this group.

IdP (SSO)-Managed Group

An identity provider (IdP) is a service that stores and verifies user identity. IdPs typically work with single sign-on (SSO) providers to authenticate users. If a user is authenticated with a SSO service of an IdP, the group information is also provided and managed by the IDP. An IdP passes the information about the user, including the user name and all the group names, where the user belongs to. Cisco SD-WAN Manager matches the group names with the group names stored in the database to further distinguish if a particular group name passed from IdP is for user group or resource group or VPN group.

Multi-Tenancy Support

With Cisco Catalyst SD-WAN multitenancy, a service provider can manage multiple customers, called tenants, from Cisco SD-WAN Manager. The tenants share Cisco SD-WAN Manager instances, Cisco SD-WAN Validator, and Cisco SD-WAN Controller. The domain name of the service provider has subdomains for each tenant. Cisco SD-WAN Manager is deployed and configured by the service provider. The provider enables multitenancy and creates a Cisco SD-WAN Manager cluster to serve tenants. Only the provider can access a Cisco SD-WAN Manager instance through the SSH terminal.

Provider has the following features:

- resource group is not applicable as the provider manages only the controllers.
- when provider provisions a new tenant, the default user account for the tenant is tenantadmin.
- other user accounts created by the provider are included in the default global resource group.
- when a provider creates a template for a tenant, the template is included in to the global resource group.

RBAC for Policies Overview

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and Cisco vManage Release 20.6.1

RBAC for policies allows a user or user group to have selective Read and Write (RW) access to Cisco SD-WAN Manager policies. For example,

- A user with RW access for Cflowd policy can only configure Cflowd policy, but cannot configure application-aware routing policy.
- A user with RW access for application aware routing policy can only configure application-aware routing policy, but cannot configure other policies.

This feature is only supported for centralized and localized policies, but not supported for security policies.

Information About Granular RBAC for Templates

Minimum supported release: Cisco vManage Release 20.7.1

When setting user group permissions, you can use the following template permissions to provide an RBAC user with a specific degree of access to different types of templates. This gives you control over the types of device configurations that an RBAC user can apply.

Permission	Description
CLI Add-On Template	Provides access to the CLI add-on feature template.
Device CLI Template	Provides access to the device CLI template.
SIG Template	Provides access to the SIG feature template and SIG credential template.
Other Feature Templates	Provides access to all feature templates except the SIG feature template, SIG credential template, and CLI add-on feature template.
Feature Profile	Provides access to all feature profiles.
Config Group	Provides access to all the configuration groups.

You can specify granular RBAC for each feature profile by expanding it. With the set permissions to the usergroup, ensure that you are able to access required feature profiles from **Templates** > **Configuration Groups**.

Single-Tenant and Multi-Tenant Scenarios

You can use granular RBAC for feature templates in single-tenant and multi-tenant Cisco SD-WAN Manager scenarios.

You can create user groups to assign specific permissions to a tenant's various teams, enabling teams to manage only specific network services without granting permission to use device CLI templates. It might be undesirable to give a tenant permission to apply device CLI templates, as the device CLI template can override any other template or device configuration.

For example, you can create a user group for a tenant's security operations group, giving them read/write access only to the SIG Template option, which would enable the security operations group to work on security configuration.

Information About Granular Configuration Task Permissions

From Cisco vManage Release 20.9.1, numerous user permission options are available, providing you fine granularity when assigning a user with permissions to manage specific configuration tasks related to configuration groups and feature profiles.

Information About Assigning Roles Locally to a User Defined by an Identity Provider

Minimum release: Cisco vManage Release 20.11.1

When you define users in an identity provider, such as Okta, for SAML SSO, one attribute that you can define for each user is the role.

When a user logs in to a Cisco SD-WAN Manager instance, Cisco SD-WAN Manager retrieves information about the user from the identity provider, including the user's role or roles. The roles defined in the identity provider map to user group permissions in Cisco SD-WAN Manager. Based on the roles of the user, Cisco SD-WAN Manager provides the user with the permissions defined by the corresponding user group.

You can assign roles locally (not depending on the identify provider) for a user profile that does not have a role defined in the identity provider.

If you have defined roles for a user through the identity provider and have also assigned user groups locally for the same user, the roles defined through the identity provider take priority.

The following table summarizes the ways to provide a user with specific permissions:

Using or Not Using an Identity Provider for SAML SSO	Roles Defined in the Identity Provider	How User Permissions Are Defined
Not using an identity provider	Not applicable	In Cisco SD-WAN Manager, assign a user to one or more user groups locally. This provides the user with the corresponding user group permissions.
Using an identity provider	Identity provider has one or more roles defined for the user.	Define roles for the user through the identity provider. Cisco SD-WAN Manager provides the user with the user group permissions corresponding to the roles.
	Identity provider does not have a role defined for the user.	Use the **Remote User** option when adding a user (**Administration** > **Manage Users** > **Add User**). See Add a User. In Cisco SD-WAN Manager, assign a user to one or more user groups locally. This provides the user with the corresponding user group permissions.

Benefits of RBAC

Benefits of Granular RBAC for Feature Templates

Minimum supported release: Cisco vManage Release 20.7.1

The permissions that you add for co-management are useful for providing detailed control over access to network configuration. They are useful when using Cisco Catalyst SD-WAN with tenants, enabling you to provide a tenant access to specific types of templates. This enables you to give the tenant self-management of network configuration tasks within the tenant's VPN.

For information about the permissions added for co-management, see Information About Granular RBAC for Templates, on page 15.

Restrictions for Role Based Access Control

General RBAC Restrictions

- Role and scope per user:

  In Cisco Catalyst SD-WAN Manager Release 20.13.1, you can only configure one role and one scope per user.

Restrictions for Application Catalog Features

- Enabling or disabling Cloud SaaS feeds:

  To enable or disable Cloud SaaS feeds, a user role requires write permission for the Application Priority Write option.

  In Cisco Catalyst SD-WAN Manager Release 20.13.x and Cisco Catalyst SD-WAN Manager Release 20.14.x, a user with the security_operations role can enable or disable Cloud SaaS feeds. From Cisco Catalyst SD-WAN Manager Release 20.15.1, the security_operations role does not include write permission for the Application Priority Write option, and does not support enabling or disabling Cloud SaaS feeds.

- Viewing discovered applications

  Discovered applications appear on the **Configuration** > **Application Catalog** > **Discovered Applications** page.

  To enable a custom role to view discovered applications, grant

  - read permission for **Cloud OnRamp**, and
  - read permission for
    - **Policy Configuration**
    - **Policy Group**
    - **Security Policy Configuration**
    - **Feature Profile** > **Embedded Security**, or
    - **Feature Profile** > **Embedded Security** > **NgFirewall**

- Creating Custom Applications

  Discovered applications appear on the **Configuration** > **Application Catalog** > **Discovered Applications** page.

  To enable a custom role to create custom applications from discovered applications, grant write permission for

  - **Policy Configuration**
  - **Policy Group**

- **Security Policy Configuration**
- **Feature Profile** > **Embedded Security**, or
- **Feature Profile** > **Embedded Security** > **NgFirewall**.

Restrictions for Granular RBAC for Feature Templates

- Template restriction options:

  To use any of the template restriction options that are provided for RBAC for co-management, provide permissions for the **Template Configuration** option. If a specific user role does not have any permissions assigned in the **Template Configuration** option, the **Templates** menu does not appear for the user in Cisco SD-WAN Manager. See Manage Users.

- Applying a template to a device:

  To enable an RBAC user to apply templates to devices, provide write permission to the **Template Deploy** option.

Use Cases for RBAC

Use Cases for Assigning Roles Locally to a User Defined by an Identity Provider

Minimum release: Cisco vManage Release 20.11.1

An organization uses the identity provider, Okta, to authenticate users logging in to Cisco SD-WAN Manager.

A user defined through the identity provider has not been assigned any roles. A network administrator with access to Cisco SD-WAN Manager, but no access to the identity provider, can locally assign the user to a specific user group to provide the user with specific permissions.

Configure Role Based Access Control

Configure Scope

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Users and Access**.

   By default **Scope** menu is selected. The table displays the list of scopes configured in the device.
2. Click **Add Scope**.
3. Enter **Scope Name** and **Description**.
4. Click **Add Nodes**.
5. Choose the required **Nodes** and click **Save**.

   (Optional) Click **Edit Nodes** to update the existing nodes in the list.
6. (Optional) In the **Associations** pane, click **Add Users** to associate users.

7. In the **Add Users** pop-up window, choose the users that you want to add.
8. Click **Save**.

   The selected users are associated to a scope.
9. (Optional) In the **Configurations** tab, click **Add Configurations** to add configurations.
10. In the **Add Configurations** page, choose the available configurations from the following tabs:
    a. **Configuration Group**
    b. **Device Template**
    c. **Feature Template**
    d. **Feature Profile**
    e. **Security Policy**
    f. **Localized Policy**
11. Click **Save**.

    A new scope with nodes, users and required configurations is created.

Configure Roles

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Users and Access**.

   By default **Roles** menu is selected. The table displays the list of scopes configured in the device.
2. Click **Add Role**.
3. Enter **Custom Role Name** in the **Add Custom Role** page.
4. Select the **Deny**, **Read**, or **Write** check box against the feature or sub feature that you want to assign a role.
5. Click **Add**.
6. You can view the new role in the table in the **Roles** page.

Copy Custom Role

1. In the list of roles, for the role you wish to copy, click **...**, and click **Copy**.

   The **Copy Custom Role** page is displayed.
2. Enter **Custom Role Name**.
3. Select the **Deny**, **Read**, or **Write** check box against the feature or sub feature that you want to update for a role.
4. Click **Copy**.
5. You can view the new role in the table in the **Roles** page.

Edit Custom Role

1. In the list of roles, for the role you wish to copy, click **...**, and click **Edit**.

   The **Edit Custom Role** page is displayed.

2. Select the **Deny**, **Read**, or **Write** check box against the feature or sub feature that you want to update for a role.
3. Click **Update**.
4. You can view the updated role in the table in the **Roles** page.

Delete a Role

You can delete a role when it is no longer needed. For example, you might delete a role that you created for a specific project when that project ends.

1. Choose the role you wish to delete, click **...**, and click **delete**.

   The **Warning** page is displayed.

2. To confirm the deletion of the role, click **Delete**.

Configure Users

Add User

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Users and Access**.
2. Click **Users**.
3. Click **Add User**.
4. Configure the following:

Field	Description
Full Name	Enter the full name of the user.
User Name	Enter the user name.
Password	Enter a password.
Remote User	Enable the **Remote User** option for remote users. If you enable this option, enter an email for the user.
Roles	Choose roles for the user.
Scope	Choose the scope for the user.
Select Locale	(Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1) Choose a locale to set the language for the Cisco SD-WAN Manager user interface.

Note In Cisco Catalyst SD-WAN Manager Release 20.12.1 and earlier releases, Cisco SD-WAN Manager only supported the English language on the user interface. From Cisco Catalyst SD-WAN Manager Release 20.13.1, Cisco SD-WAN Manager user interface supports Canadian French.

5. Click **Add** to add the user.

Edit User

1. In the **Users** page, for the user you wish to edit, click **...**, and click **Edit**.

   The **Edit User** page is displayed.
2. Enter **Full Name**, **User Name**.
3. Choose the role from the **Roles** drop-down list.
4. Choose the scope from the **Scope** drop-down list.
5. (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1) Choose the locale from the **Select Locale** drop-down list.
6. Click **Update**.

Copy User

1. For the user you wish to copy, click **...**, and click **Copy**.

   The **Copy User** page is displayed.
2. Enter **Full Name**, **User Name**.
3. Enter the password in the **Password** and **Confirm Password**fields.
4. Choose the role from the **Roles** drop-down list.
5. Choose the scope from the **Scope** drop-down list.
6. (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1) Choose the locale from the **Select Locale** drop-down list.
7. Click **Copy**.

Delete User

If a user no longer needs access to devices, you can delete the user. Deleting a user does not log out the user if the user is logged in.

1. For the user you wish to delete, click **...**, and click **Delete**.
2. To confirm the deletion of the user, click **OK**.

Change User Password

1. For the user you wish to change the password, click **...** and click **Change Password**.

2. Enter the **Current User Password**.
3. Enter the new password in the **Password** field.
4. Enter the new password again in the **Confirm Password** field.
5. Click **Update**.

Reset Locked User

1. For the user you wish to reset the lock, click **...** and click **Reset Locked User**.
2. In the **Reset Locked User** pop-up menu, click **Yes**.

Administrative Lock

1. For the user you wish to reset the lock, click **...** and click **Administrative Lock**.
2. In the **Lock User** pop-up menu, click **Yes**.

Configure User Sessions

User Sessions page shows a list of all the active HTTP sessions within Cisco SD-WAN Manager, including username, domain, source IP address, and so on.

To remove a user session, choose the session from the list, and click **Remove Session**.

Verify RBAC

Verify Granular RBAC Permissions

Minimum supported release: Cisco vManage Release 20.7.1

Use this procedure to verify the permissions that you have configured for a user group.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Manage Users**.
2. Click **User Groups**.
3. In the pane that displays the user groups, select a user group to display the read and write permissions assigned to the user group.
4. Scroll to the permissions that control template access to verify your configuration for the user group.

Monitor RBAC

Monitor devices for VPN Groups

To monitor devices:

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Click **WAN - Edge**.
3. Select the **VPN Group** and **VPN Segment** for which you want to monitor the network.

   A web page displays the list of VPN groups and segments that are configured to a device.