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 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.

Restriction for Role Based Access Control

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

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**.