

Network Hierarchy and Resource Management

Table 1: Feature History

Feature Name	Release Information	Description
Network Hierarchy and Resource Management	Cisco SD-WAN Release 20.9.1 Cisco vManage Release 20.9.1	This feature enables you to create a network hierarchy in Cisco SD-WAN Manager to represent the geographical locations of your network. The network hierarchy and the associated resource IDs, including region IDs and site IDs, help you apply configuration settings to a device. In addition, the introduction of the resource manager in Cisco SD-WAN Manager automatically manages these resource IDs, thereby simplifying the overall user experience of Cisco Catalyst SD-WAN. Note that you can create a region only if you enable the **Multi-Region Fabric** option in Cisco SD-WAN Manager.
Network Hierarchy and Resource Management (Phase II)	Cisco IOS XE Catalyst SD-WAN Release 17.10.1a Cisco vManage Release 20.10.1	The following enhancements are introduced in the Network Hierarchy and Resource Management feature. • Creation of a system IP pool on the **Configuration** > **Network Hierarchy** page • Automatic assignment of site ID, system IP, and hostname to a device in the Quick Connect workflow • Display of detailed information on the **Configuration** > **Network Hierarchy** page, including site ID pool, region ID pool, and the list of devices associated with a site
Support for Software Defined Remote Access Pools	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	Remote access refers to enabling secure access to an organization's network from devices at remote locations. The resource pool manager manages the IPv4 and IPv6 private IP address pools for Cisco Catalyst SD-WAN remote access devices. You can create a software defined remote access pool using the **Configuration** > **Network Hierarchy** page.

Feature Name	Release Information	Description
Support for Traffic Flow Collectors	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	This feature enables you to configure traffic flow collectors such as the Cflowd server and security logging server. Cflowd monitors service side traffic flowing through devices in the overlay network and exports flow information to the collector. Enable security logging and configure servers for high-speed logging (HSL) and collecting external syslogs. You can configure the traffic flow collectors by navigating to **Configuration** > **Network Hierarchy** > **Collectors**.

- Information About Network Hierarchy and Resource Management, on page 2
- Supported Devices for Network Hierarchy and Resource Management, on page 3
- Restrictions for Network Hierarchy and Resource Management, on page 3
- Manage a Network Hierarchy, on page 4
- Assign Resource IDs to Devices, on page 13
- Configure Collectors in a Network Hierarchy, on page 16

Information About Network Hierarchy and Resource Management

Overview of Network Hierarchy

You can create a network hierarchy in Cisco SD-WAN Manager to represent the geographical locations of your network. Your network hierarchy can contain three types of nodes—regions, areas, and sites. The resource IDs assigned to the nodes help you identify where to apply configuration settings later.

By default, there is one node called global in the network hierarchy.

The network hierarchy has a predetermined hierarchy with three types of nodes:

- Region: It represents a region in a multiregion fabric-based Cisco Catalyst SD-WAN deployment. The Multi-Region Fabric feature provides the option to divide the architecture of the Cisco Catalyst SD-WAN overlay network into multiple regional networks that operate distinctly from one another, and a central core-region network for managing inter-regional traffic.

  You can create a region only if you enable the **Multi-Region Fabric** option in Cisco SD-WAN Manager. For complete information about the Multi-Region Fabric feature, see the *Cisco Catalyst SD-WAN Multi-Region Fabric (also Hierarchical SD-WAN) Configuration Guide*.

- Group/Area: A group, also called an area, is a logical grouping of nodes in a network hierarchy. You can group sites, regions, other areas, or any combination of these into an area.

- Site: A site is the lowest level of node or the leaf node in a network hierarchy. You cannot create a child node under a site. You can only associate devices to a site.

For complete information about creating and managing different nodes in a network hierarchy, see Manage a Network Hierarchy.

Overview of Resource Management

The resource manager in Cisco SD-WAN Manager manages the resource IDs, that is, region IDs and site IDs. It automatically generates a region ID for a region that you create on the **Configuration** > **Network Hierarchy** page. Similarly, it generates a site ID for a site if you do not specify it.

You can assign a site ID and a region ID to a device. For complete information about assigning resource IDs to devices, see Assign Resource IDs to Devices.

If you upgrade from an earlier version of Cisco SD-WAN Manager to Cisco vManage Release 20.9.1, the resource manager in Cisco SD-WAN Manager automatically creates sites based on the site IDs of the existing devices in your setup. Sites are named as SITE_<*id*>. Cisco SD-WAN Manager displays these sites under the global node on the **Network Hierarchy** page. It also associates the existing devices with their sites in the network hierarchy.

Benefits of Network Hierarchy and Resource Management

- Automates the management of regions and sites.
- Saves the manual effort in an upgrade scenario when Cisco SD-WAN Manager discovers all your existing sites and displays them in the network hierarchy.
- Simplifies the onboarding and configuration of devices.
- Monitors and collects information about traffic flow.

Supported Devices for Network Hierarchy and Resource Management

This feature is supported on Cisco IOS XE Catalyst SD-WAN devices and Cisco vEdge devices.

Restrictions for Network Hierarchy and Resource Management

- You can delete a node only if it does not have any child node. For example, you can delete a site only if no devices are associated with it.
- A site is the lowest level of a node or the leaf node in a network hierarchy. You cannot create a child node under a site.
- You cannot create more than one region node between the global node and a site node.
- You cannot create a region in a multitenant deployment.
- The maximum combined number of regions and secondary regions is 63 (region ID numbers 1 through 63).

Manage a Network Hierarchy

The Network Hierarchy and Resource Management feature enables you to do the following:

- Create a region
- Create an area
- Create, edit, and delete a site

Create a Region in a Network Hierarchy

Before You Begin

(For Cisco Catalyst SD-WAN Manager Release 20.12.x or earlier) Ensure that the **Multi-Region Fabric** option in Cisco SD-WAN Manager is enabled. See Enable Multi-Region Fabric in the *Cisco Catalyst SD-WAN Multi-Region Fabric Configuration Guide*.

From Cisco Catalyst SD-WAN Manager Release 20.13.1, configuring regions is enabled by default. It does not require enabling Multi-Region Fabric.

Create a Region, Cisco Catalyst SD-WAN Manager Release 20.13.1 and Later

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy**.
2. Click **…** adjacent to **Global** in the left pane and choose **Add Node**.
3. Do one of the following:
   - If Multi-Region Fabric is not enabled:

     In the **Add Node** pop-up window, check the **Behave as SDWAN Region** checkbox.

     If you do not check this checkbox, this procedure creates a new group within the network hierarchy instead of a region.
   - If Multi-Region Fabric is enabled:

     In the **Add Node** pop-up window, choose **Region**.
4. Configure the following:

Field	Description
Name	Name for the region. The name must be unique and can contain only letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.).
Description	Description of the region.
Parent drop-down list	Choose a parent node.

5. Click **Add**.

The new region appears in the left pane.

6. (Optional) You can click a region name or a secondary region name in the left pane to display the automatically assigned region ID number. The region ID number appears above the table in the right pane. The maximum combined number of regions and secondary regions is 63 (region ID numbers 1 through 63).

Create a Region, Cisco Catalyst SD-WAN Manager Release 20.12.x or Earlier

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy**.
2. Click **…** adjacent to a node (global or area) in the left pane and choose **Add MRF Region**.

Note In Cisco vManage Release 20.9.x, you can also use the **Add Node** option to add a region.

3. In the **Name** field, enter a name for the region. The name must be unique and can contain only letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.).
4. In the **Description** field, enter a description of the region.
5. From the **Parent** drop-down list, choose a parent node.
6. Click **Add**.

Create a Subregion in a Network Hierarchy

Note From Cisco IOS XE Catalyst SD-WAN Release 17.15.1a and Cisco Catalyst SD-WAN Control Components Release 20.15.1, configuration of this feature is supported only through API.

Before You Begin

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1

- From Cisco Catalyst SD-WAN Manager Release 20.13.1, configuring subregions is enabled by default. It does not require enabling Multi-Region Fabric.
- Create a region before creating a subregion. See Create a Region in a Network Hierarchy, on page 4.
- For the maximum combined number of regions and secondary regions, see Restrictions for Network Hierarchy and Resource Management, on page 3.

Create a Subregion

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy**.
2. Click **…** adjacent to a region in the left pane and choose **Add MRF Sub Region**.
3. In the **Add Sub-Region** pop-up window, configure the following:

Field	Description
Name	Name for the region. The name must be unique and can contain only letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.).
Description	Description of the region.
Parent	This field is automatically populated with the region to which you are adding the subregion, and is not configurable.

4. Click **Add**.

   The new subregion appears in the left pane.

Create a Secondary Region in a Network Hierarchy



Note From Cisco IOS XE Catalyst SD-WAN Release 17.15.1a and Cisco Catalyst SD-WAN Control Components Release 20.15.1, configuration of this feature is supported only through API.

Before You Begin

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1

- Create a region before creating a subregion. See Create a Region in a Network Hierarchy, on page 4.
- For the maximum combined number of regions and secondary regions, see Restrictions for Network Hierarchy and Resource Management, on page 3.

Create a Secondary Region

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy**.
2. Click **…** adjacent to **Global** in the left pane and choose **Add Node**.
3. In the **Add Node** pop-up window, click **Secondary Region**.
4. Configure the following:

Field	Description
Name	Name for the region. The name must be unique and can contain only letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.).
Description	Description of the region.
Parent	This field shows **Secondary Regions**, and is not configurable.

5. Click **Add**.

The new secondary region appears in the left pane, in the **Secondary Regions** section.

6. (Optional) You can click a region name or a secondary region name in the left pane to display the automatically assigned region ID number. The region ID number appears above the table in the right pane. The maximum combined number of regions and secondary regions is 63 (region ID numbers 1 through 63).

Create a Group in a Network Hierarchy

Before You Begin

In Cisco Catalyst SD-WAN Manager Release 20.12.x and earlier, a group is called an area.

Create a Group

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy**.
2. Click **…** adjacent to a node (global, region, or group) in the left pane and choose **Add Node.**
3. In the **Add Node** pop-up window, in the **Type** field, choose **Group**.

   (In Cisco Catalyst SD-WAN Manager Release 20.12.x and earlier, choose **Add Area**.



Note In Cisco vManage Release 20.9.x, you can also use the **Add Node** option to add an area.

4. In the **Name** field, enter a name for the group. The name must be unique and can contain only letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.).
5. In the **Description** field, enter a description of the group.
6. From the **Parent** drop-down list, choose a parent node.
7. Click **Add**.

Create a Site in a Network Hierarchy

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy**.
2. Click **…** adjacent to a node (global, region, or area) in the left pane and choose **Add Site**.



Note In Cisco vManage Release 20.9.x, you can also use the **Add Node** option to add a site.

3. In the **Name** field, enter a name for the site. The name must be unique and can contain only letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.).
4. In the **Description** field, enter a description of the site.
5. From the **Parent** drop-down list, choose a parent node.

6. In the **Site ID** field, enter a site ID.

   If you do not enter the site ID, Cisco SD-WAN Manager generates a site ID for the site.

7. In the **Address** field, enter the address.

   When you enter an address, latitude and longitude fields are auto populated.

8. In the **Latitude** field, enter the latitude of the site.

9. In the **Longitude** field, enter the longitude of the site.

10. Click **Add**.



Note The **Address** , **Latitude**, and **Longitude** fields are included starting from Cisco IOS XE Catalyst SD-WAN Release 17.18.1a. When you type in the address, the latitude and longitude fields are auto-populated.

Conversely, you can also enter your own latitude and longitude. If a corresponding location is found, then the address field will be auto-populated. If you do not want to provide address data for your site, then you can check the **Undisclosed Address** check box.

Field	Description
Name	Enter a name for the site. The name must be unique and can contain only letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.).
Description	Enter a description of the site.
Parent	From the drop-down list, choose a parent node.
Site ID	Enter a site ID. If you do not enter the site ID, Cisco SD-WAN Manager generates a site ID for the site.
Address	Enter the address. When you enter an address, latitude and longitude fields are auto populated.
Latitude	Specifies latitude of the site. When you enter the latitude of the site, the address field is auto populated if the location of the site is found.
Longitude	Specifies longitude of the site. When you enter the longitude of the site, the address field is auto populated if the location of the site is found.

Edit a WAN Region

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy**.
2. Click **…** adjacent to the region name and choose **Edit WAN Region**.

In releases earlier than Cisco Catalyst SD-WAN Manager Release 20.15.1, choose **Edit MRF Region**.

3. Edit the options as needed. You can edit the name, description, and parent of the region.
4. Click **Save**.

Delete a WAN Region

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy**.
2. Click **…** adjacent to the region name and choose **Delete WAN Region**.

   In releases earlier than Cisco Catalyst SD-WAN Manager Release 20.15.1, choose **Delete MRF Region**.
3. In the confirmation dialog box, click **Yes**.

Edit a Group

Before You Begin

In Cisco Catalyst SD-WAN Manager Release 20.12.x and earlier, a group is called an area.

Edit a Group

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy**.
2. Click **…** adjacent to the group name and choose **Edit Group**.

   (In Cisco Catalyst SD-WAN Manager Release 20.12.x and earlier, choose **Edit Area**.
3. Edit the options as needed. You can edit the name, description, and parent of the group.
4. Click **Save**.

Delete a Group

Before You Begin

In Cisco Catalyst SD-WAN Manager Release 20.12.x and earlier, a group is called an area.

Delete a Group

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy**.
2. Click **…** adjacent to the group name and choose **Delete Group**.

   (In Cisco Catalyst SD-WAN Manager Release 20.12.x and earlier, choose **Delete Area**.
3. In the confirmation dialog box, click **Yes**.

Edit a Site

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy**.
2. Click **…** adjacent to the site name and choose **Edit Site**.
3. Edit the options as needed. You can edit only the name, description, and parent of the site.
4. Click **Save**.

Note After reassigning a site to a different region in the **Network Hierarchy Manager**, follow the procedures in the sections Assign a Site ID to a Device and Assign a Region ID to a Device to ensure configuration updates are properly applied to the affected device.

Delete a Site

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy**.
2. Click **…** adjacent to the site name and choose **Delete Site**.
3. In the confirmation dialog box, click **Yes**.

Create a System IP Pool

Minimum releases: Cisco IOS XE Catalyst SD-WAN Release 17.10.1a, Cisco vManage Release 20.10.1

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy**.

   The page displays the site pool and region pool for the Global node.
2. Click **Pools**.
3. Click **Add Pool**.
4. In the **Pool Name** field, enter a name for the pool.
5. In the **Pool Description** field, enter a description of the pool.
6. From the **Pool Type** drop-down list, choose **System IP**.
7. In the **IP Subnet*** field, enter an IP address.
8. In the **Prefix Length*** field, enter the prefix length of the system IP pool.
9. Click **Add**.

Note You can create only one system IP pool. If you want to make any changes to the pool, you must edit the existing pool.

Edit a System IP Pool

Minimum releases: Cisco IOS XE Catalyst SD-WAN Release 17.10.1a, Cisco vManage Release 20.10.1

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy**.

   The page displays the site pool and region pool for the Global node. The system IP pool is also displayed if you have already created it.

2. Click **…** adjacent to the system IP name and choose **Edit**.
3. Edit the options as needed.

Note You can only expand the pool range and cannot enter a lower IP address than the already specified IP address.

4. Click **Save**.

Create a Remote Access Pool

Minimum supported release: Cisco vManage Release 20.11.1

The resource pool manager supports creation of IPv4 and IPv6 private IP pools for Cisco Catalyst SD-WAN remote access devices. In the remote access configuration you can select the remote access private IP Pool by defining the number of IP addresses.

For more information on Software Defined Remote Access, see Cisco Catalyst SD-WAN Remote Access.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy**.

   The page displays the site pool and region pool for the Global node.

2. Click **Add Pool**.
3. In the **Pool Name** field, enter a name for the pool.
4. In the **Pool Description** field, enter a description of the pool.
5. From the **Pool Type** drop-down list, choose **Remote Access**.
6. Choose the **IP Type** by clicking the radio button next to **IPv4** or **IPv6**.
7. In the **IP Subnet** field, enter an IP subnet.
8. In the **Prefix Length** field, enter the prefix length of the remote access pool.
9. Click **Add**.

Edit a Remote Access Pool

Minimum supported release: Cisco vManage Release 20.11.1

You can edit a remote access pool only when you want to expand the pool range.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy**.

The page displays the site pool and region pool for the Global node. The remote access pool is also displayed if you have already created it.

2. Click **…** adjacent to the remote access pool name and choose **Edit**.
3. Edit the options as needed.



Note When you edit a remote access pool, the new pool range cannot be less than the existing pool range

4. Click **Save**.

Create an IP Pool for ThousandEyes

SUMMARY STEPS

1. From the menu, choose **Configuration** > **Network Hierarchy**.
2. Examine the audit logs to determine if the ThousandEyes test has been posted or failed.
3. Click **Pools**.
4. Click **Add Pool**.
5. In the **Pool Name** field, enter a name for the pool.
6. In the **Pool Description** field, enter a description of the pool.
7. From the **Pool Type** drop-down list, choose **ThousadEyes**.
8. In the **IP Subnet*** field, enter an IP address.
9. In the **Prefix Length*** field, enter the prefix length of the system IP pool.
10. Click **Add**.

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	From the menu, choose **Configuration** > **Network Hierarchy**.	The page displays the site pool and region pool for the Global node.
Step 2	Examine the audit logs to determine if the ThousandEyes test has been posted or failed.	
Step 3	Click **Pools**.	
Step 4	Click **Add Pool**.	
Step 5	In the **Pool Name** field, enter a name for the pool.	
Step 6	In the **Pool Description** field, enter a description of the pool.	
Step 7	From the **Pool Type** drop-down list, choose **ThousadEyes**.	
Step 8	In the **IP Subnet*** field, enter an IP address.	

	Command or Action	Purpose
Step 9	In the **Prefix Length*** field, enter the prefix length of the system IP pool.	
Step 10	Click **Add**.	

Delete a Pool

Minimum supported release: Cisco vManage Release 20.11.1

1. From the Cisco SD-WAN Manager menu, choose **Configuration > Network Hierarchy**.
2. In the Global page, click **…** adjacent to the pool name and choose **Delete**.
3. In the confirmation dialog box, click **Yes**.



Note You can delete a pool only when the pool resources are not in use.

Assign Resource IDs to Devices

The Network Hierarchy and Resource Management feature enables you to do the following:

- Assign a site ID to a device
- Assign a region ID to a device

Assign a Site ID to a Device

You can assign a site ID to a device using one of the following ways.

Use the Quick Connect Workflow

1. From the Cisco SD-WAN Manager menu, choose **Workflows** > **Workflow Library**.
2. Start the **Quick Connect** workflow.
3. Follow the instructions provided in the workflow.
4. On the **Add and Review Device Configuration** page, enter the site ID of the device.

Note

- You can use any of the existing site IDs that are available in the network hierarchy or enter a new site ID. If you enter a new site ID without creating a node in the network hierarchy, the site is automatically created and listed on the **Configuration** > **Network Hierarchy** page.
- (Minimum releases: Cisco IOS XE Catalyst SD-WAN Release 17.10.1a, Cisco vManage Release 20.10.1) If you want Cisco SD-WAN Manager to automatically generate a site ID for the device, do not make any change to the default value, **AUTO**.

Use a Template

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices** > **WAN Edge List**.
2. Check if a device is attached to a device template.
3. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** > **Feature Templates**.
4. Click **…** adjacent to the System feature template and choose **Edit**.
5. Click the **Basic Configuration** tab and set the scope of the **Site ID** field to **Global** and enter the site ID.
6. Click **Update**.
7. Click **Configure Devices** to push the configuration to the device.

In Step 5, if you set the scope of the **Site ID** field to **Device Specific**, do the following:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** > **Device Templates**.
2. Click **…** adjacent to the device template and choose **Edit Device Template**.
3. In the **Site ID** field, enter the site ID.

   You can use any of the existing site IDs that are available in the network hierarchy or enter a new site ID. If you enter a new site ID without creating a node in the network hierarchy, the site is automatically created and listed on the **Configuration** > **Network Hierarchy** page.
4. Click **Update**.
5. Click **Configure Devices** to push the configuration to the device.

Use a Configuration Group

The configuration group flow is applicable only for the Cisco IOS XE Catalyst SD-WAN devices.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** > **Configuration Groups**.
2. Click **…** adjacent to the configuration group name and choose **Edit**.
3. Click **Associated Devices**.
4. Choose a device that is associated with the configuration group and click **Deploy**.

   The **Deploy Configuration Group** workflow starts.
5. Follow the instructions provided in the workflow.

6. On the **Add and Review Device Configuration** page, enter the site ID of the device.

   You can use any of the existing site IDs that are available in the network hierarchy or enter a new site ID. If you enter a new site ID without creating a node in the network hierarchy, the site is automatically created and listed on the **Configuration** > **Network Hierarchy** page.

Assign a Region ID to a Device

Before You Begin

- Have access to the **Multi-Region Fabric** feature.
- Ensure that the region is available in the network hierarchy.

Assign a Region ID

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices** > **WAN Edge List**.
2. Check if the corresponding device is attached to a device template.
3. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** > **Feature Templates**.
4. Click **…** adjacent to the System feature template and choose **Edit**.
5. Click the **Basic Configuration** tab and set the scope of the **Region ID** field to **Global** and enter the region ID.

   You can use any of the existing region IDs that are available in the network hierarchy. If the specified region ID is not available in the network hierarchy, the template push operation to the devices fails.
6. Click **Update**.
7. Click **Configure Devices** to push the configuration to the device.

In Step 5, if you set the scope of the **Region ID** field to **Device Specific**, do the following:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** > **Device Templates**.
2. Click **…** adjacent to the device template and choose **Edit Device Template**.
3. In the **Region ID** field, enter the region ID.
4. Click **Update**.
5. Click **Configure Devices** to push the configuration to the device.

Assign a System IP to a Device

Minimum releases: Cisco IOS XE Catalyst SD-WAN Release 17.10.1a, Cisco vManage Release 20.10.1

1. From the Cisco SD-WAN Manager menu, choose **Workflows** > **Workflow Library**.
2. Start the **Quick Connect** workflow.
3. Follow the instructions provided in the workflow.

4. On the **Add and Review Device Configuration** page, enter the system IP of the device. If you want Cisco SD-WAN Manager to automatically generate a system IP for the device, do not make any change to the default value, **AUTO**.

Assign a Hostname to a Device

Minimum releases: Cisco IOS XE Catalyst SD-WAN Release 17.10.1a, Cisco vManage Release 20.10.1

1. From the Cisco SD-WAN Manager menu, choose **Workflows** > **Workflow Library**.
2. Start the **Quick Connect** workflow.
3. Follow the instructions provided in the workflow.
4. On the **Add and Review Device Configuration** page, enter the hostname of the device. If you want Cisco SD-WAN Manager to automatically generate a hostname for the device, do not make any change to the default value, **AUTO**.

Configure Collectors in a Network Hierarchy

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, Cisco Catalyst SD-WAN Manager Release 20.13.1.

Configure Cflowd and security logging servers that help monitor traffic flow and collect information about service-side traffic.

Information About Collectors

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, Cisco Catalyst SD-WAN Manager Release 20.13.1.

Collectors process traffic flowing through routers in the overlay network and export flow information to a server. The collectors maintain information about the flow and data that is extracted from the IP headers of the packets in the traffic flow.

You can configure the location of cflowd collectors, how often sets of sampled flows are sent to the collectors, and how often the samples are sent to the collectors (on Cisco SD-WAN Controllers only). You can configure a maximum of four cflowd collectors per Cisco IOS XE Catalyst SD-WAN Device. To have a cflowd configuration take effect, apply it with the appropriate data policy.

Configure Cflowd

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, Cisco Catalyst SD-WAN Manager Release 20.13.1.

Before You Begin

You can configure the location of cflowd collectors, how often sets of sampled flows are sent to the collectors, and how often the samples are sent to the collectors (on Cisco SD-WAN Controllers only). You can configure

a maximum of four cflowd collectors per Cisco IOS XE Catalyst SD-WAN device. To have a cflowd configuration take effect, apply it with the appropriate data policy.

Ensure that you specify the granular role-based access control (RBAC) for Cflowd and policy groups. With specific permissions to the user group, ensure that you are able to access policy groups from **Configuration** > **Policy Groups**. For more information about configuring RBAC for policy groups, see Configure RBAC for policy groups in Prerequisites for Policy Groups.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Users and Access** > **Roles**.
2. Click **Edit** next to existing roles or click **Add Role** to create a new role.
3. Choose the desired permission for the **Cflowd** feature under **Network Settings** and click **Update**.

Configure Cflowd

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy** > **Collectors**.
2. Enable Cflowd and configure the values in the following table for the collector server:

Field	Description
Add Collector Server	
VPN ID	VPN ID of the server. Range: 1 to 65525, excluding 512. For details see the VRF range behavior change described here.
IPv4/IPv6 Address	IPv4 or IPv6 address of the collector server.
UDP Port	UDP port number of the collector server. Range: 1024 through 65535
Export Spreading	Toggle to enable or disable the export spreading configuration.
BFD Metrics Exporting	Toggle to enable or disable Bidirectional Forwarding Detection (BFD) metrics.
Exporting Interval	Interval in seconds for sending BFD metrics. **Exporting Interval** appears if you have enabled **BFD Metrics Exporting**. The default BFD export interval is 600 seconds.
Advanced Settings	
Active Flow Timeout (Seconds)	Active flow timeout value. Range: 30 through 3600 Default: 600 seconds.
Inactive Flow Timeout (Seconds)	Inactive flow timeout value. Range: 1 through 3600 Default: 60 seconds.

Field	Description
Flow Refresh Time (Seconds)	Flow refresh time in seconds. Range: 60 through 86400 seconds. Default: 600 seconds.
Sampling Rate	Sample duration in seconds. Range: 1 through 65536. Default: 1 second.
Collect TLOC Loopback	Enable to collect information about the TLOC loopback.
Protocol	Traffic protocol type to apply the collector to. The options are: **IPv4**, **IPv6**, or **both**. The default protocol is **IPv4**.
TOS	Type of field in the IPv4 header.
Re-marked DSCP	Traffic output of the router's data policy.

You can configure up to four collector servers.

3. Click **Save**.

The Cflowd settings that you configure are applied to the application priority and SLA policy when the policy is deployed to Cisco Catalyst SD-WAN devices. You can monitor application traffic flow over IPv4, IPv6, or both network addresses. For more information about configuring additional settings, see **Monitor traffic flow** in Application Priority and SLA.

Configure Security Logging

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, Cisco Catalyst SD-WAN Manager Release 20.13.1.

Configure Security Logging

You can set up security logging for Cisco IOS XE Catalyst SD-WAN devices by configuring the location of the destination IP address of the log server. You can configure up to four destination servers along with the source interface to collect the syslogs for High Speed Logging (HSL). The IP address for the destination server can be IPv4, IPv6, or both. For more information about configuring HSL, see Configure Firewall High-Speed Logging Using the CLI Template. You can configure the external syslog server to export UTD logs. For more information about UTD logging, see Create Unified Security Policy Summary page.

Before You Begin

Ensure that you specify the granular role-based access control (RBAC) for security logging. Ensure that you are able to access policy groups from **Configuration** > **Policy Groups** by configuring specific permissions to the user group. For more information about configuring RBAC for policy groups, see "Configure RBAC for policy groups" in Prerequisites for Policy Groups.

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

2. Click **Edit** adjacent to existing roles or click **Add Role** to create a new role.
3. Choose the permission you wish to configure for the **Security Logging** feature under **Network Settings** and click **Update**.

Configure Security Logging

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy** > **Collectors**.
2. Enable **Security Logging** and configure the values in the following table for the high-speed logging and external syslog servers:

Field	Description
High Speed Logging	Configure the following values for the high-speed logging server: • **VPN**: VPN name of the high-speed logging server. The VPNs available in the drop-down list are ones that are previously configured in the configuration groups in Cisco SD-WAN Manager. • **Server IP**: IPv4 or IPv6 address of the log collector server. • **Port**: Port number on which the log collector server is listening for incoming packets.
External Syslog Server	Configure the following values for the external syslog server: • **VPN**: VPN name of the external syslog server. The VPNs available in the drop-down list are ones that are previously configured in the configuration groups in Cisco SD-WAN Manager. • **Server IP**: IPv4 or IPv6 address of the external syslog server.

You can configure up to four high-speed logging servers.



Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.16.1a and Cisco Catalyst SD-WAN Manager Release 20.16.1, server labels (**Server 1**, **Server 2**, **Server 3**, and **Server 4**) are added to the high-speed logging server and the syslog server.

For device-specific server settings, add the associated source interface in the **Additional Settings** of the NGFW policy. For more information about configuring additional settings in the policy groups, see Configure NGFW Additional Settings section.

For Global server settings, define the global NHM values. For more information about defining global values on NHM, see Network Hierarchy and Resource Management.

3. Click **Save**.

The security logging settings that you configure are applied along with the embedded security policy when the policy is deployed to Cisco Catalyst SD-WAN devices. For more information about configuring the embedded security policy, see Configure Embedded Security.