

Cisco Catalyst SD-WAN Network Hierarchy Configuration Guide, Releases 26.x and Later

Cisco SD-WAN
Updated September 28, 2026

© 2026 Cisco Systems, Inc. All rights reserved.

Full Cisco Trademarks with Software License

Full Cisco Trademarks with Software License

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.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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: https://www.cisco.com/c/en/us/about/legal/trademarks.html. 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. (1721R)

Topics included

1 Network Hierarchy Management....5

Feature history for network hierarchy management....6
Network hierarchy management....7
Benefits of network hierarchy....7
Supported devices for network hierarchy....8
Restrictions for network hierarchy....8
Manage a network hierarchy....8
Create a region in a network hierarchy....8
Create a subregion in a network hierarchy....9
Create a secondary region in a network hierarchy....10
Create a group in a network hierarchy....11
Create a site in a network hierarchy....11
Edit a WAN region....12
Delete a WAN region....12
Edit a group....13
Delete a group....13
Edit a site....13
Delete a site....13
Create a system IP pool....14
Edit a system IP pool....14
Create a remote access pool....15
Edit a remote access pool....15
Create an IP pool for ThousandEyes....16
Delete a pool....16

2 Resource Management and Collectors in a Network Hierarchy....17

Feature history of resource management and collectors....18
Resource management and collectors....18
Assign resource IDs to devices....19
Assign a site ID to a device using the quick connect workflow....19
Assign a site ID to a device using a template....19
Assign a site ID to a device using a configuration group....20
Assign a region ID to a device....20
Assign a system IP to a device....21
Assign a hostname to a device....21
Configure cflowd....22
Configure security logging....23

1 Network Hierarchy Management

Topics:

- Feature history for network hierarchy management
- Network hierarchy management
- Benefits of network hierarchy
- Supported devices for network hierarchy
- Restrictions for network hierarchy
- Manage a network hierarchy

Defines the logical framework used to organize network nodes into geographical or logical groupings and explains the hierarchy structure of regions, areas, and sites.

Feature history for network hierarchy management

Provides a chronological summary of feature releases, including updates to network hierarchy, resource management, and traffic flow collectors.

Table 1: Feature History

Feature Name	Release Information	Description
Network Hierarchy	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a 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. You can create a network hierarchy in Cisco SD-WAN Manager to represent the geographical locations of your network. You can create a region, an area, and a site in a network hierarchy. In addition, you can assign a site ID and a region ID to a device.
Network Hierarchy Enhancement	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 You can create a system IP pool on the **Configuration** > **Network Hierarchy** page.
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.
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**.

Feature Name	Release Information	Description
End of Support for Secondary Regions and Subregions	Cisco IOS XE Catalyst SD-WAN Release 17.15.1a Cisco Catalyst SD-WAN Manager Release 20.15.1	This release ends support for secondary regions and subregions.

Network hierarchy management

Defines the logical framework used to organize network nodes into geographical or logical groupings and explains the hierarchy structure of regions, areas, and sites.

A network hierarchy is a logical framework in Cisco SD-WAN Manager that

- organizes network nodes into geographical or logical groupings,
- assigns resource IDs to each node to assist with configuration management, and
- establishes a predetermined multi-level structure supporting regions, areas, and sites.

By default, there is one node called global in the network hierarchy. The network hierarchy has a predetermined hierarchy with three types of nodes.

- A region is a top-level node in a multiregion fabric-based Cisco Catalyst SD-WAN deployment. Regions segment the SD-WAN overlay into distinct networks and require the Multi-Region Fabric feature to be enabled.

  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): An area, also called a group, is a logical grouping of nodes such as sites, regions, or other areas. Areas allow flexible organization of network locations within the hierarchy.
- Site: A site is the lowest-level node in the hierarchy. Sites represent specific network locations and can be associated with network devices. Child nodes cannot be created under a site.
- By default, the hierarchy includes a single global node.
- Resource IDs assigned to nodes help determine where to apply configuration settings in Cisco SD-WAN Manager.
- To create or manage nodes in a network hierarchy, see "Manage a Network Hierarchy" in the product documentation.

Benefits of network hierarchy

Outlines the advantages of the hierarchy, such as automated management, simplified device onboarding, and improved traffic flow monitoring.

These are the benefits of network hierarchy.

- 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

Identifies that the network hierarchy feature is supported on Cisco IOS XE Catalyst SD-WAN devices.

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

Restrictions for network hierarchy

Details the operational limitations, including node deletion rules, hierarchy depth constraints, and maximum region limits.

These are the restrictions for network hierarchy.

- 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

Provides step-by-step procedures for creating, editing, and deleting various nodes, including regions, subregions, secondary regions, groups, and sites.

Create a region in a network hierarchy

Use these steps to create a Region for Cisco Catalyst SD-WAN Manager Release 20.12.1 and 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**
   >
   > 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**.

(For Cisco Catalyst SD-WAN Manager Release 20.12.1 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. Use these steps to create a Region for Cisco Catalyst SD-WAN Manager Release 20.13.1 and later.

Procedure

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 subregion in a network hierarchy

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 section.

- For the maximum combined number of regions and secondary regions, see Restrictions for Network Hierarchy and Resource Management.

Procedure

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 and , configuration of this feature is supported only through API.

Before you begin

- Create a region before creating a subregion.
- For the maximum combined number of regions and secondary regions.

Procedure

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

Procedure

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**.
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

Procedure

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**.
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. n the **Latitude** and **Longitude** fields, enter the latitude longitude values of the site.
9. Click **Add**.

   Use the following table to enter the fields.

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.

Field	Description
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.

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.

Edit a WAN region

Procedure

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

Procedure

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

3. In the confirmation dialog box, click **Yes**.

Edit a group

Procedure

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

Delete a group

Procedure

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

Edit a site

Procedure

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**.

What to do next

Note

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

Delete a site

Procedure

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

Explains the process for defining a system IP pool on the Network Hierarchy page.

Procedure

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

Outlines how to modify the range of an existing system IP pool.

Procedure

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

Describes the steps to set up IPv4 or IPv6 private IP address pools for remote access devices.

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.

Procedure

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

Details the procedure for updating the range of an existing remote access pool.

Procedure

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

Provides instructions for configuring a specific IP pool to support ThousandEyes testing.

Procedure

1. From the menu, choose **Configuration** > **Network Hierarchy**. The page displays the site pool and region pool for the Global node.
2. Examine the audit logs to determine if the ThousandEyes test has been posted or failed.
3. Click **Pools** and 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 **ThousadEyes**.
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**.

Delete a pool

Explains the conditions and steps required to remove an unused IP pool from the system.

Procedure

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.

2 Resource Management and Collectors in a Network Hierarchy

Topics:

- Feature history of resource management and collectors
- Resource management and collectors
- Assign resource IDs to devices
- Assign a region ID to a device
- Assign a system IP to a device
- Assign a hostname to a device
- Configure cflowd
- Configure security logging

Guides through resource management concepts and procedures for assigning identifiers, configuring network devices, and implementing logging mechanisms within hierarchical network structures.

Feature history of resource management and collectors

Lists the development milestones and release information for he Resource Management and Traffic Flow Collector features. This table describes the developments of this feature, by release.

Table 2: Feature History

Feature Name	Release Information	Description
Resource Management	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a 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. You can create a network hierarchy in Cisco SD-WAN Manager to represent the geographical locations of your network. You can create a region, an area, and a site in a network hierarchy. In addition, you can assign a site ID and a region ID to a device.
Resource Management Enhancement	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	The following enhancements are introduced in the 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 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**.

Resource management and collectors

Explains how the resource manager automatically generates and manages region and site IDs to simplify network hierarchy organization.

The resource manager in Cisco SD-WAN Manager manages resource IDs, which include region IDs and site IDs. The resource manager automatically generates a region ID when you create a region 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.

When you upgrade from an earlier version of Cisco SD-WAN Manager to Cisco vManage Release 20.9.1, the resource manager automatically creates sites based on the site IDs of your devices. Each site is named SITE_. The sites appear under the global node on the **Configuration** > **Network Hierarchy** page, and Cisco SD-WAN Manager associates each device with its site in the network hierarchy.

Collectors

Collectors process traffic that flows through routers in the overlay network and export flow information to a server. They maintain flow data extracted from the IP headers of packets within the traffic.

You can configure the location of cflowd collectors and set how frequently sampled flows are sent to the collectors. The samples are sent to the collectors at specific intervals. 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.

Assign resource IDs to devices

Outlines the methods for assigning site IDs, region IDs, system IPs, and hostnames to devices using workflows, templates, or configuration groups.

The resource management feature enables you to assign site ID, region ID, system IP, and host names to a device.

Assign a site ID to a device using the quick connect workflow

Procedure

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.
> - 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**.

Assign a site ID to a device using a template

Procedure

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.

   If you set the scope of the **Site ID** field to **Device Specific**, do the following:

   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** > **Device Templates**.

   b. Click **...** adjacent to the device template and choose **Edit Device Template**.

   c. 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.

   d. Click **Update**.

   e. Click **Configure Devices** to push the configuration to the device.

6. Click **Update**.
7. Click **Configure Devices** to push the configuration to the device.

Assign a site ID to a device using a configuration group

Procedure

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

Details the prerequisites and steps required to associate a device with a specific region within the network hierarchy.

Before you begin

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

Procedure

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.

   If you set the scope of the **Region ID** field to **Device Specific**, do the following:

   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** > **Device Templates**.

   b. Click **...** adjacent to the device template and choose **Edit Device Template**.

   c. In the **Region ID** field, enter the region ID.

   d. Click **Update**.

   e. Click **Configure Devices** to push the configuration to the device.

6. Click **Update**.
7. Click **Configure Devices** to push the configuration to the device.

Assign a system IP to a device

Describes how to use the Quick Connect workflow to manually or automatically assign a system IP to a device.

Procedure

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

Explains the process of using the Quick Connect workflow to assign a custom or automatically generated hostname to a device.

Procedure

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 cflowd

Covers the requirements and procedures for enabling Cflowd to monitor service-side traffic and export flow data to collector servers.

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**.

Procedure

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: 0 through 65536
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.

Field	Description
Inactive Flow Timeout (Seconds)	Inactive flow timeout value. Range: 1 through 3600 Default: 60 seconds.
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 IOS XE 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

Details how to set up high-speed logging (HSL) and external syslog servers to collect and export security-related logs from devices.

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). You can provide an IPv4 or IPv6 address for each destination server. 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**.

Procedure

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/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/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 IOS XE Catalyst SD-WAN devices. For more information about configuring the embedded security policy, see Configure Embedded Security.