Cisco Catalyst SD-WAN Integrations

First Published: 2024-08-27

Last Modified: 2025-08-20

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

CHAPTER 1

Read Me First

Note To achieve simplification and consistency, the Cisco SD-WAN solution has been rebranded as Cisco Catalyst SD-WAN. In addition, from Cisco IOS XE SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Release 20.12.1, the following component changes are applicable: **Cisco vManage** to **Cisco Catalyst SD-WAN Manager**, **Cisco vAnalytics** to **Cisco Catalyst SD-WAN Analytics**, **Cisco vBond** to **Cisco Catalyst SD-WAN Validator**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

Related References

- Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Server Recommendations
- Cisco Catalyst SD-WAN Device Compatibility

User Documentation

- User Documentation for Cisco IOS XE Catalyst SD-WAN Release 17

Communications, Services, and Additional Information

- Sign up for Cisco email newsletters and other communications at: Cisco Profile Manager.
- For information on the latest technical, advanced, and remote services to increase the operational reliability of your network visit Cisco Services.
- To browse and discover secure, validated enterprise-class apps, products, solutions, and services, visit Cisco Devnet.
- To obtain general networking, training, and certification titles from Cisco Press Publishers, visit Cisco Press.
- To find warranty information for a specific product or product family, visit Cisco Warranty Finder.
- To view open and resolved bugs for a release, access the Cisco Bug Search Tool.
- To submit a service request, visit Cisco Support.

Documentation Feedback

To provide feedback about Cisco technical documentation use the feedback form available in the right pane of every online document.

CHAPTER 2

What's New in Cisco IOS XE (SD-WAN) and Cisco Catalyst SD-WAN Releases

Cisco is constantly enhancing the Cisco Catalyst SD-WAN solution with every release and we try and keep the content in line with the latest enhancements. The following links includes release-wise new and modified features that are documented in the Configuration, Command Reference, and Hardware Installation guides. For information on additional features and fixes that were committed to the Cisco Catalyst SD-WAN solution, see the *Resolved and Open Bugs* section in the Release Notes.

What's New in Cisco IOS XE Catalyst SD-WAN Release 17.x

What's New in Cisco IOS XE Catalyst SD-WAN Release 16.x

What's New in Cisco SD-WAN (vEdge) Release 20.x

What's New in Cisco SD-WAN (vEdge) Release 19.x

CHAPTER 3

Cisco Cyber Vision Integration with Cisco Catalyst SD-WAN

Cisco Cyber Vision Integration with Cisco Catalyst SD-WAN

Table 1: Feature History

Feature Name	Release Information	Feature Description
Cisco Cyber Vision Integration	Cisco IOS XE Catalyst SD-WAN Release 17.15.1a Cisco Catalyst SD-WAN Control Components Release 20.15.1 Cisco Cyber Vision Center Release 5.0.0	Cisco SD-WAN Manager supports integration with the Cisco Cyber Vision network security solution. You can configure devices in the network to monitor and inspect traffic on one or more interfaces and send traffic metadata or a copy of your network traffic to Cisco Cyber Vision Center to analyze it for security concerns.

Information About Cisco Cyber Vision Integration

Cisco SD-WAN Manager supports integration with Cisco Cyber Vision, which is a network security solution. Cisco Cyber Vision provides visibility into the security status of your global network, indicates when devices in the network require attention to maintain a secure posture, helps you to configure security policies, and more. The browser-based manager is called Cisco Cyber Vision Center. Documentation for Cisco Cyber Vision is available here.

Value of the Integration

The integration enables you to use Cisco SD-WAN Manager to configure devices in the network to operate as software-based sensors. Acting as a sensor is a functional value add to devices such as routers or switches. Sensors are an integral part of what enables Cisco Cyber Vision to manage security threats in the network.

You can configure devices acting as sensors to monitor and inspect traffic on one or more interfaces, and to send traffic metadata to Cisco Cyber Vision Center to analyze it for security concerns. Alternatively, you can send a copy of your network traffic to Cyber Vision Center for centralized monitoring and inspection. Note that sending a copy of your network traffic uses more network resources than sending only metadata.

Cisco Cyber Vision Application

In contrast with many features that you can enable on network devices, Cisco Cyber Vision functionality is not included as part of a Cisco IOS XE Catalyst SD-WAN software release.

When you enable Cisco Cyber Vision on a device, the device downloads and installs the Cisco Cyber Vision application. This is a Cisco IOx application that operates in a Docker container. As with other Cisco IOx applications, it operates together with Cisco IOS XE Catalyst SD-WAN to provide additional functionality.

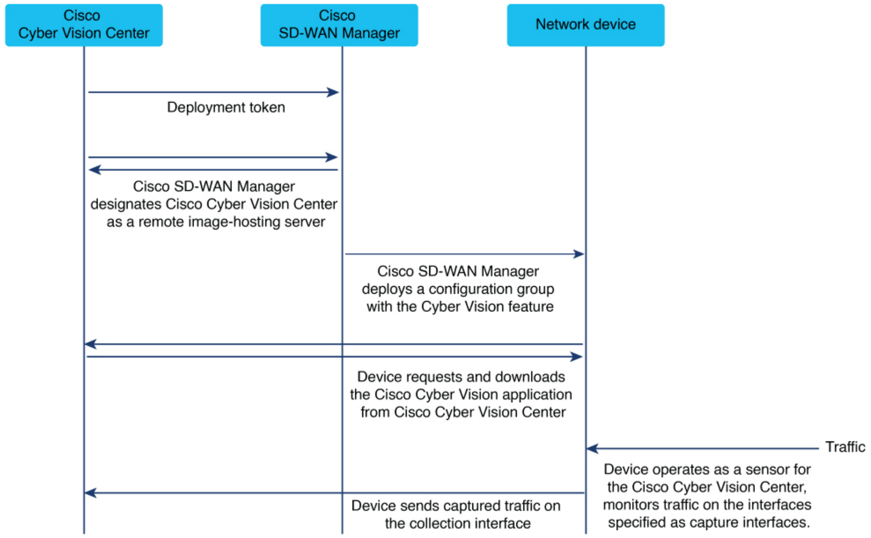
After a successful installation, the device operates as a sensor for Cisco Cyber Vision. The device appears in the sensor list in Cisco Cyber Vision Center.

How Devices Download and Install the Cisco Cyber Vision Application

For the integration with Cisco Cyber Vision, Cisco SD-WAN Manager designates the Cisco Cyber Vision Center as a remote image-hosting server for the Cisco Cyber Vision application.

Overview of the Application Installation Process

Figure 1: Integration of Cisco Cyber Vision and Cisco Catalyst SD-WAN


Cisco Cyber Vision Center
Cisco SD-WAN Manager
Network device
Deployment token
Cisco SD-WAN Manager designates Cisco Cyber Vision Center as a remote image-hosting server
Cisco SD-WAN Manager deploys a configuration group with the Cyber Vision feature
Device requests and downloads the Cisco Cyber Vision application from Cisco Cyber Vision Center
Traffic
Device operates as a sensor for the Cisco Cyber Vision Center, monitors traffic on the interfaces specified as capture interfaces.
Device sends captured traffic on the collection interface

1. As described in the Configure a Connection to a Cisco Cyber Vision Center in the Network Hierarchy, on page 10 procedure prerequisites, you log in to Cisco Cyber Vision Center and generate a type of token called a deployment token.

2. When you complete the Configure a Connection to a Cisco Cyber Vision Center in the Network Hierarchy, on page 10 procedure, Cisco SD-WAN Manager uses the information in the deployment token to designate the Cisco Cyber Vision Center as the host for the Cisco Cyber Vision application.

   To designate Cisco Cyber Vision Center as the host from which to download the application, Cisco SD-WAN Manager adds Cisco Cyber Vision Center as a remote server. As such, it appears on the **Maintenance** > **Software Repository** page, in the **Remote server** tab. As described in Guidelines for Cisco Cyber Vision Integration, on page 9, do not edit or remove the server.

3. When you push a Cisco Cyber Vision configuration to devices in the network, the devices connect to Cisco Cyber Vision Center to download the Cisco Cyber Vision application.

4. The devices install and activate the application. This enables the devices to operate as sensors for the Cisco Cyber Vision Center.

Using Cisco Cyber Vision Center

The procedures described here enable devices to operate as sensors for the Cisco Cyber Vision Center. After you've set this up, use Cisco Cyber Vision Center to monitor the security of the network you are managing with Cisco Catalyst SD-WAN. For information, see the latest Cisco Cyber Vision GUI Administration Guide.

Supported Platforms for Cisco Cyber Vision Integration

Table 2: Supported Platforms

Platform series	Models	Supported from
Cisco Catalyst IR1100 Rugged Series	IR 1101	Cisco Catalyst SD-WAN Control Components Release 20.15.1
Cisco Catalyst IR1800 Rugged Series	IR1821 IR1831 IR1833 IR1835	Cisco Catalyst SD-WAN Control Components Release 20.16.1

Prerequisites for Cisco Cyber Vision Integration

Cisco Cyber Vision Center Version

Cisco Cyber Vision Center Release 5.0.0 or later

Network Reachability to Cisco Cyber Vision Center

Ensure that devices in the network have network reachability to Cisco Cyber Vision Center before deploying a configuration group that includes the Cisco Cyber Vision feature.

Because of this requirement, configuring devices to work with Cisco Cyber Vision Center is a two-step process:

1. Deploying a configuration group to a set of devices to establish reachability to Cisco Cyber Vision Center.
2. Deploying a configuration group to a set of devices to enable Cisco Cyber Vision on the devices.

   After you confirm reachability in the previous step, you can modify the same configuration group that you used in that step, adding the Cisco Cyber Vision feature, and deploy the configuration group to the devices.

This same requirement applies when you add devices to a configuration group that has the Cisco Cyber Vision feature and that you have deployed to devices already. If you want to deploy the configuration group to additional devices, make note of the above and first establish reachability to Cisco Cyber Vision Center for the additional devices.

Virtual port groups

The Cisco Cyber Vision application requires virtual port group (VPG) interfaces 5 and 6 to be available. Ensure that these VPG interfaces are not configured for use with a different application.

Guidelines for Cisco Cyber Vision Integration

Do not remove remote servers

Cisco SD-WAN Manager adds one or more Cisco Cyber Vision Center instances as servers on the **Maintenance** > **Software Repository** page, in the **Remote server** tab.

Do not edit or remove these remote servers.

Restrictions for Cisco Cyber Vision Integration

Cisco IOx application limitation

If a device is running the Cisco Cyber Vision application, it cannot run other Cisco IOx applications.

Cannot onboard a device to Cisco Cyber Vision Center more than once using the same token

This restriction applies only to Cisco Catalyst SD-WAN Manager Release 20.15.x.

As described in Configure a Connection to a Cisco Cyber Vision Center in the Network Hierarchy, on page 10, Cisco SD-WAN Manager uses a deployment token created in Cisco Cyber Vision to establish a secure link (called a connection in the procedure) with Cisco Cyber Vision Center. You can configure more than one such connection between Cisco SD-WAN Manager and Cisco Cyber Vision Center.

When using Cisco Catalyst SD-WAN Manager Release 20.16.x, you can onboard a device in the network to Cisco Cyber Vision Center only one time using a single deployment token.

If you uninstall a device from a Cisco Cyber Vision Center instance, you need to use a new token to redeploy the device to that same Cisco Cyber Vision Center instance. In Cisco SD-WAN Manager, this means using a new connection to Cisco Cyber Vision Center.

Moving devices from one Cisco Cyber Vision Center instance to another requires uninstalling the Cyber Vision application from the devices

This restriction applies to Cisco Catalyst SD-WAN Manager Release 20.15.x and Cisco Catalyst SD-WAN Manager Release 20.16.x.

If you have onboarded devices to an instance of Cisco Cyber Vision and you need to move them to a different instance of Cisco Cyber Vision, you need to first push a configuration to the devices that does not include the Cyber Vision feature. This results in uninstalling the Cyber Vision application from the devices. Next, push a new configuration to the devices that specifies the new Cisco Cyber Vision instance.

Multitenancy

- In Cisco Catalyst SD-WAN Manager Release 20.15.x and 20.16.x, multitenant environments do not support integration with Cisco Cyber Vision.
- From Cisco Catalyst SD-WAN Manager Release 20.18.1, multitenant environments support integration with Cisco Cyber Vision only at the tenant level, not at the provider level.

Configure Cisco Cyber Vision Integration, High Level

Procedure

Step 1 Configure a Connection to a Cisco Cyber Vision Center in the Network Hierarchy, on page 10

Step 2 Create a Configuration Group Profile with a Cyber Vision Feature, on page 11

Step 3 Add a Cyber Vision Feature to a Configuration Group, on page 13

Step 4 Deploy a Configuration Group with a Cisco Cyber Vision Feature, on page 14

What to do next

After the configuration steps, you can monitor the activity of the Cisco Cyber Vision application operating on a device. See Monitor the Cisco Cyber Vision Application on Devices, on page 17.

Configure a Connection to a Cisco Cyber Vision Center in the Network Hierarchy

Before you begin

- Deployment token

  In Cisco Cyber Vision Center, create one or more deployment tokens to enable devices to establish a secure link with Cisco Cyber Vision Center. This table indicates the token type required, according to the supported platform type.

  Table 3: Required Token Type by Platform

Platform	Token Type
Cisco Catalyst IR1101 Rugged Series	cviox-aarch64.tar

  For information about creating a deployment token, see the latest Cisco Cyber Vision GUI Administration Guide.

  Copy the token text and have it ready for the procedure.

- Connectivity

  The devices in your network that operate with Cisco Cyber Vision require network reachability to the Cisco Cyber Vision Center. Ensure that your network topology provides this reachability.

Procedure

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

Step 2 Click **External Services**.

Step 3 In the **Cyber Vision** pane, click **Add Cyber Vision Center**.

Step 4 In the table of Cisco Cyber Vision connections, enter these:

Field	Description
Name	Name of the Cisco Cyber Vision Center.
IP Address or Hostname	IP address of the server hosting the Cisco Cyber Vision Center. **Note** Entering a hostname is not supported.
Token	Paste in the deployment token that you copied from the Cisco Cyber Vision Center, as noted in the prerequisites.
VPN	VPN by which devices in the network connect to the Cisco Cyber Vision Center.

Step 5 Click **Save**.

Using information contained in the token, Cisco SD-WAN Manager automatically sets up a server as one of the remote image-hosting servers that appear on the **Maintenance** > **Software Repository** page, in the **Remote server** tab. See How Devices Download and Install the Cisco Cyber Vision Application, on page 6.

Create a Configuration Group Profile with a Cyber Vision Feature

Before you begin

On the **Configuration** > **Configuration Groups** page, choose either

- **SD-WAN**, or
- **SD-Routing**

as the solution type.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure a Cyber Vision feature in an Other profile.

a. Enter a name and description for the feature.

Table 4: Name and Description

Field	Description
Name	Name for the Cisco Cyber Vision Center.

Field	Description
Description	Optionally, add a description.

b. Configure the base configuration fields.

Table 5: Base Configuration

Field	Description
Cyber Vision Center	From the drop-down list, choose a Cisco Cyber Vision Center connection from the list of previously configured connections. See Configure a Connection to a Cisco Cyber Vision Center in the Network Hierarchy.
Monitoring Source Interface	Click **Add** and enter the interface for the device to use for monitoring traffic. Your choice depends on your network and the traffic that you want the device to monitor. Examples: VLAN interface, cellular interface, WAN interface

c. The **Advanced Configuration** area appears only if you are configuring a **Cyber Vision** feature for the **SD-WAN** solution option. It does not appear for the **SD-Routing** solution option.

The fields in this area are preconfigured to use variables that enable you to enter device-specific information for each device when deploying the configuration group. See Deploy a Configuration Group with a Cisco Cyber Vision Feature, on page 14. But you can configure global device values instead of using the variables.

Table 6: Advanced Configuration

Field	Description
Capture Interface IP	IP address of the interface that captures the traffic for analysis.
Capture Interface Subnet Mask	Subnet mask for the interface that captures the traffic for analysis.
Collection Interface (Sensor to Center) IP	Enter an IP address for the collection interface that sends the captured traffic to Cisco Cyber Vision Center. Ensure that the IP address is within the subnet mask defined in the **Collection Interface Subnet Mask** field. **Note** For each device connecting to Cisco Cyber Vision Center through the same service VPN, enter a unique collection interface IP address. It is necessary for each interface within a single service VPN to use a unique IP address. To view the service VPN configured for communication with Cisco Cyber Vision Center, see Configure a Connection to a Cisco Cyber Vision Center in the Network Hierarchy.
Collection Interface Subnet Mask	Subnet mask for the collection interface that sends the captured traffic to Cisco Cyber Vision Center. The subnet mask defines an address space for the service VPN used for communication between device and Cisco Cyber Vision Center.

Field	Description
VPG5 (Virtual Port Group) IP Address	IP address within the subnet mask defined in the **Collection Interface Subnet Mask** field. This is an address with the same network as the collection interface. **Note** For each device connecting to Cisco Cyber Vision Center through the same service VPN, enter a unique VPG5 IP address. It is necessary for each interface within a single service VPN to use a unique IP address.
VPG6 (Virtual Port Group) IP Address	This field is preset and not configurable.

What to do next

Also see Deploy a configuration group.

Add a Cyber Vision Feature to a Configuration Group

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 In the solution drop-down list, choose either

- **SD-WAN**, or
- **SD-Routing**

as the solution type to display configuration groups only for this solution.

Step 3 Click the **Configuration Groups** tab.

Step 4 If you need to create a configuration group, follow the steps described in Using Configuration Groups in *Cisco Catalyst SD-WAN Configuration Groups*.

Step 5 For an existing configuration group, click **Add Profile** and add an **Other Profile** to the configuration group.

Step 6 In the configuration group, locate the **Other Profile** drop-down list and choose a Cisco Cyber Vision profile.

Deploy a Configuration Group with a Cisco Cyber Vision Feature

Before you begin

- See Supported Platforms for Cisco Cyber Vision Integration, on page 8 before deploying a configuration group with the Cisco Cyber Vision feature.
- Ensure that devices in the network have network reachability to Cisco Cyber Vision Center before deploying a configuration group that includes the Cisco Cyber Vision feature. This requires two steps:

  1. Deploy a configuration group to establish reachability to Cisco Cyber Vision Center.
  2. Deploy a configuration group to enable Cisco Cyber Vision on the devices.

     After you confirm reachability in the previous step, you can modify the same configuration group that you used in that step, adding the Cisco Cyber Vision feature, and deploy the configuration group to the devices.

  See Prerequisites for Cisco Cyber Vision Integration, on page 8.

Note This same requirement applies when you add devices to a configuration group that has the Cisco Cyber Vision feature and that you have deployed to devices already. If you want to deploy the configuration group to additional devices, make note of the above and first establish reachability to Cisco Cyber Vision Center for the additional devices.

Procedure

Step 1 Use the standard configuration group deployment procedure in *Cisco Catalyst SD-WAN Configuration Groups* to deploy a configuration group to devices in the network.

Step 2 If you are deploying to devices of the SD-WAN solution type, during deployment, enter these device-specific variables, in the **CV_SDWAN** pane, for each router.

If you are deploying to devices of the SD-Routing solution type, skip this step.

Field	Description
collection_int_ip	Enter an IP address for the collection interface that sends the captured traffic to Cisco Cyber Vision Center. Ensure that the IP address is within the subnet mask defined in the **collection_int_subnet** field. **Note** For each device connecting to Cisco Cyber Vision Center through the same service VPN, enter a unique collection interface IP address. It is necessary for each interface within a single service VPN to use a unique IP address. To view the service VPN configured for communication with Cisco Cyber Vision Center, see Configure a Connection to a Cisco Cyber Vision Center in the Network Hierarchy, on page 10.
collection_int_subnet	Subnet mask for the collection interface that sends the captured traffic to Cisco Cyber Vision Center. The subnet mask defines an address space for the service VPN used for communication between device and Cisco Cyber Vision Center.
vpg5_ip	IP address within the subnet mask defined in the **collection_int_subnet** field. This is an address with the same network as the collection interface. **Note** For each device connecting to Cisco Cyber Vision Center through the same service VPN, enter a unique VPG5 IP address. It is necessary for each interface within a single service VPN to use a unique IP address.

Step 3 If you want to monitor the progress of installing the Cisco Cyber Vision application on a device, view the log messages for the installation.

a. Click the task list button near the top right.

b. Click the **Deploy configuration group** task.

This opens a page showing the deployment progress for each device.

c. Adjacent to a device, click the log icon in the **Action** column.

The **View Logs** pane opens, showing the deployment progress for the device. When the deployment is complete, and when the devices have established a connection to the Cisco Cyber Vision server, a success message, such as "Config Group successfully deployed to device," appears in the log.

When you first deploy a configuration group with the Cisco Cyber Vision feature to a device, it triggers the device to install the Cisco Cyber Vision application. It takes several minutes for a device to install the Cisco Cyber Vision application. After a successful installation, the device operates as a sensor for Cisco Cyber Vision. The device appears in the sensor list Cisco Cyber Vision Center. For information about verifying this, see Verify that Cisco SD-WAN Manager Has Connected to the Cisco Cyber Vision Center, on page 16.

Verify that Cisco SD-WAN Manager Has Connected to the Cisco Cyber Vision Center

When you create a configuration group with a Cisco Cyber Vision feature, deploying the configuration group to devices triggers the devices to install the Cisco Cyber Vision application. It takes several minutes for a device to install the Cisco Cyber Vision application. After a successful installation, the device operates as a sensor for Cisco Cyber Vision. The device appears in the sensor list Cisco Cyber Vision Center. See Cisco Cyber Vision Application.

Before you begin

Deploy a configuration group with a Cisco Cyber Vision feature to one or more devices. See Deploy a Configuration Group with a Cisco Cyber Vision Feature, on page 14.

Procedure

Step 1 Log in to the Cisco Cyber Vision Center.

Step 2 View the active sensors. For details, see the latest Cisco Cyber Vision GUI Administration Guide.

Each device appears separately in the list of sensors.

Verify that the Cisco Cyber Vision Application is Operating on a Device, Using the CLI

This verification method is applicable to devices in the SD-WAN or SD-Routing solutions.

Before you begin

Deploy a configuration group with a Cisco Cyber Vision feature to one or more devices. See Deploy a Configuration Group with a Cisco Cyber Vision Feature, on page 14.

Procedure

Step 1 On a device running the Cisco Cyber Vision application, run this command.

```
Device# show iox-service
```

Step 2 Based on the output of the command in the previous step, do one of these:

- If the command output shows that the IOxman service is running, then proceed to the next step.

- If the command output shows that the IOxman service is not running, this indicates that the Cisco Cyber Vision application is not operating correctly. Reinstall the application. See Deploy a Configuration Group with a Cisco Cyber Vision Feature, on page 14.

Step 3 On the same device, run this command. If the output shows that state as running, this indicates that the Cisco Cyber Vision application is operating correctly.

```
Device# show app-hosting detail appid cv
```

Example

In this example, the Cisco Cyber Vision application is installed and operating. Note that the command output is truncated here.

```
Device# show iox-service
IOx Infrastructure Summary:
IOx service (CAF)              : Running
IOx service (HA)               : Not Supported
IOx service (IOxman)           : Running
IOx service (Sec storage)      : Running
Libvirtd 5.5.0                 : Running
Dockerd v19.03.13-ce           : Running

Device# show app-hosting detail appid cv
App id                 : cv
Owner                  : iox
State                  : RUNNING
...
```

Monitor the Cisco Cyber Vision Application on Devices

Before you begin

Deploy a configuration group with a Cisco Cyber Vision feature to one or more devices. See Deploy a Configuration Group with a Cisco Cyber Vision Feature, on page 14.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

Step 2 Click a device name for a device in the SD-WAN solution.

Note
This monitoring method is applicable to devices in the SD-WAN solution, but not to devices in the SD-Routing solution.

Step 3 Click the **Real Time** tab.

Step 4 Enter any of these App Hosting commands in the **Device Options** field to view the resource usage or other details of the Cisco Cyber Vision application operating on the device:

- App Hosting Details

- App Hosting Utilization
- App Hosting Network Utilization
- App Hosting Storage Utilization
- App Hosting Processes
- App Hosting Attached Devices
- App Hosting Network Interfaces
- App Hosting Guest routes

CHAPTER 4

Cisco Secure Equipment Access integration with Cisco Catalyst SD-WAN

Cisco Secure Equipment Access integration with Cisco Catalyst SD-WAN

Table 7: Feature history

Feature name	Release information	Feature description
Cisco Secure Equipment Access integration	Cisco IOS XE Catalyst SD-WAN Release 17.16.1a Cisco Catalyst SD-WAN Manager Release 20.16.1	Cisco Secure Equipment Access (SEA) is a solution that provides remote access to network-connected assets. Assets can include anything reachable by IP address, such as servers, industrial internet of things (IIoT) devices, and so on. Integration with Cisco Catalyst SD-WAN enables you to use Cisco SD-WAN Manager to deploy the Cisco SEA solution within a Cisco Catalyst SD-WAN network.

Information about Cisco Secure Equipment Access integration

Cisco Secure Equipment Access (SEA) is a solution that provides remote access to network-connected assets. Assets can include anything reachable by IP address, such as servers, industrial internet of things (IIoT) devices, and so on. Integration with Cisco Catalyst SD-WAN enables you to use Cisco SD-WAN Manager to

- install the SEA agent on devices, such as routers, in the Cisco Catalyst SD-WAN overlay network
- configure connectivity between the devices in the overlay network and the Cisco Secure Equipment Access cloud portal, and
- configure how remote assets connect to the devices.

After you install the SEA agent on devices and configure the connectivity described here, other remote access tasks operate as usual for Cisco SEA. See Secure Equipment Access Overview on the Cisco DevNet site.

Benefits of Cisco Secure Equipment Access integration

Remote access is important for configuring, managing, and troubleshooting operational technology (OT) assets without time-consuming and costly site visits. Cisco Secure Equipment (SEA) combines all the benefits of a Zero-Trust Network Access (ZTNA) solution with a network architecture that makes it simple to deploy at scale in operational environments. There is no dedicated hardware to install and manage, or complex firewall rules to configure and maintain. It features comprehensive security capabilities, with advanced cybersecurity controls and easy-to-build policies based on identities and contexts.

Cisco SEA provides numerous benefits:

- Operational efficiency

  Enables operations teams easy remote access to OT assets, even those behind NAT boundaries.

- Simple installation and scalability

  Operates through existing routers and switches, so there is no need for dedicated appliances or complex firewall setups.

- Strong security controls

  Authenticates users with MFA and SSO. Cisco SEA verifies each user's security posture, providing access only to relevant assets.

- Least-privilege access

  Allows select users to access only specific devices, using only certain protocols, and only at defined times.

- Audit trail

  Records sessions and builds audit trails for investigation and compliance.

Cisco Secure Equipment Access application

Installing the SEA agent

A Cisco IOx application called the Cisco Secure Equipment Access (SEA) agent provides Cisco SEA functionality to a device (a router in the network). When you enable Cisco SEA on a device through Cisco SD-WAN Manager, the device downloads and installs the Cisco SEA application.

Cisco SEA cloud portal

After a successful installation of the Cisco SEA agent, the device communicates with the Cisco SEA cloud portal. It appears in the device list in the Cisco SEA cloud portal.

Using the Cisco Secure Equipment Access solution

The procedures described here enable devices to operate as part of the Cisco Secure Equipment Access solution. After you've set this up, use Cisco SEA to manage access to remote assets. For information, see the Cisco Secure Equipment Access documentation on the Cisco DevNet site.

Supported platforms for Cisco Secure Equipment Access integration

Table 8: Supported platforms

Platform series	Models
Cisco Catalyst IR1100 Rugged Series Routers	Cisco Catalyst IR1101
Cisco Catalyst IR1800 Rugged Series Routers	Cisco Catalyst IR1821 Cisco Catalyst IR1831 Cisco Catalyst IR1833 Cisco Catalyst IR1835

Prerequisites for Cisco Secure Equipment Access integration

Network reachability to the Cisco Secure Equipment Access portal

Before deploying a configuration group that includes the Cisco SEA feature, ensure that the routers in the network that will run the Cisco SEA agent application have network reachability to the Cisco SEA cloud portal.

Because of this requirement, configuring devices to work with Cisco SEA is a two-step process:

1. Deploying a configuration group to a set of devices to establish reachability to a Cisco SEA cloud portal.
2. Deploying a configuration group to a set of devices to enable Cisco SEA on the devices.

   After you confirm reachability in the previous step, you can modify the same configuration group that you used in that step, adding the Cisco SEA feature, and deploy the configuration group to the devices.

This same requirement applies when you add devices to a configuration group that has the Cisco SEA feature and that you have deployed to devices already. If you want to deploy the configuration group to additional devices, make note of the above and first establish reachability to a Cisco SEA cloud portal for the additional devices.

Virtual port group interfaces

The Cisco SEA application requires virtual port group (VPG) interfaces 7 to 10 to be available. Ensure that these VPG interfaces are not configured for use with a different application.

The Cisco SEA application uses VPG interface 7 to connect to the Cisco SEA cloud portal, and reserves VPG interfaces 8 to 10 to connect to remote assets. For restrictions that apply to virtual port groups, see Restrictions for Cisco Secure Equipment Access integration, on page 22.

IP address for virtual port group interface 7

For each router, configure an IP address for VPG interface 7 connectivity to the Cisco SEA cloud portal.

Restrictions for Cisco Secure Equipment Access integration

Single Cisco SEA cloud portal

Cisco SD-WAN Manager can connect to only a single Cisco SEA cloud portal.

Single Cisco SD-WAN Manager

A single organization, as defined in the Cisco SEA cloud portal, can connect to only one Cisco SD-WAN Manager. This has consequences for a Cisco SEA cloud portal that is operating in a multitenant environment, because a Cisco SD-WAN Manager instance represents a single organization.

Virtual port groups (VPG) and remote asset connectivity

The Cisco SEA application uses VPG interface 7 to connect to the Cisco SEA cloud portal, and reserves VPG interfaces 8 to 10 to connect to assets. A single VPG interface (8, 9, or 10) can provide connectivity for a single remote asset network. The remote asset network can include more than one asset.

Editing Secure Equipment Access Cloud fields

On the **Configuration** > **Network Hierarchy** > **External Services** page, in the **Secure Equipment Access Cloud** section, if you update the **VPN** or **Proxy** fields, Cisco SD-WAN Manager resets the IP address of the remote server called SEA-RemoteServer.

If you edit these fields, restore the IP address of the remote server:

1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository** > **Remote server**.

2. Edit the remote server for SEA to use the locally hosted remote server that you have configured.
   a. Edit the automatically created server, called: SEA-RemoteServer
   b. Change the IP address to use the locally hosted remote server that hosts the SEA Agent image.

API key

The API key used for establishing a secure link with the Cisco SEA cloud portal has an expiration period of one year.

Remote server

In Cisco Catalyst SD-WAN Manager Release 20.16.x, the Cisco SEA Agent image is locally hosted on a remote server using HTTP protocol only. SCP and FTP protocols are not supported.

Multitenancy

- In Cisco Catalyst SD-WAN Manager Release 20.16.x, multitenant environments do not support integration with Cisco Secure Equipment Access.
- From Cisco Catalyst SD-WAN Manager Release 20.18.1, multitenant environments support integration with Cisco Secure Equipment Access only at the tenant level, not at the provider level.

Configure Cisco Secure Equipment Access integration, high level

Procedure

Step 1 Configure a connection to a Cisco Secure Equipment Access portal in the Network Hierarchy, on page 24

Step 2 Upload the Cisco SEA application to Cisco SD-WAN Manager, on page 25

Step 3 Create a Configuration Group Profile with an SEA Feature, on page 26

Step 4 Add a Cisco SEA Feature to a Configuration Group, on page 29

Step 5 Deploy a Configuration Group with a Cisco SEA Feature, on page 30

What to do next

After the configuration steps, you can monitor the activity of the Cisco SEA application operating on a device. See Monitor the Cisco Secure Equipment Access application on devices, on page 32.

Configure a connection to a Cisco Secure Equipment Access portal in the Network Hierarchy

Configure a secure connection between your network devices and the Cisco Secure Equipment Access (SEA) cloud portal within the Network Hierarchy using Cisco SD-WAN Manager.

Before you begin

API key

1. In the Cisco SEA cloud portal, create an API key to enable devices to establish a secure link with the Cisco SEA cloud portal.

   For information about creating an API key, see the Cisco Secure Equipment Access documentation on the Cisco DevNet site. When you generate the API key, if there is an option to enable the key for external controller integration, choose that option.

2. Copy the API key and have it ready for the procedure.

Connectivity

The devices in your network that operate with Cisco SEA require network reachability to the Cisco SEA cloud portal. Ensure that your network topology provides this reachability.

Remote server

In Cisco Catalyst SD-WAN Manager Release 20.16.x, set up a remote server. This is a locally hosted file server, required to host the Cisco SEA Agent image. See Register Remote Server for setup instructions.

Procedure

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

Step 2 Click **External Services**.

Step 3 In the **Secure Equipment Access Cloud** pane, enter these:

Table 9: Secure Equipment Access Cloud Pane

Field	Description
Cluster access type	Choose an API key option: • **Manual**: Enter the API key manually by copying it from the Cisco SEA cloud portal. • **Auto**: Retrieve the API key automatically from the Cisco SEA cloud portal.
API Key	(This field appears if you choose **Manual** in **Cluster access type**.) Enter the API key that you generated in the Cisco SEA cloud portal.

Field	Description
Select Secure Equipment Access Cluster	(This field appears if you choose **Auto** in **Cluster access type**.) Choose the cluster name associated with your Cisco SEA cloud portal account. Click **Connect** and log in with your Cisco SEA cloud portal credentials.
VPN	VPN providing reachability between devices and the Cisco SEA cloud portal. **Note** If you later edit this field, see the restriction regarding editing Secure Equipment Access Cloud fields, in Restrictions for Cisco Secure Equipment Access integration, on page 22.
Proxy	If devices in your network require a proxy for connectivity between devices and the Cisco SEA cloud portal, enter the IP address of the proxy. **Note** If you later edit this field, see the restriction regarding editing Secure Equipment Access Cloud fields, in Restrictions for Cisco Secure Equipment Access integration, on page 22.

Step 4 Click **Save**.

Step 5 If you are using Cisco Catalyst SD-WAN Manager Release 20.16.x, do this:

a) Open **Maintenance** > **Software Repository** > **Remote server**.

b) Edit the automatically created remote server called: SEA-RemoteServer to use the locally hosted remote server that you have configured.

c) Change the IP address to use the locally hosted remote server that hosts the SEA Agent image.

Note
From Cisco Catalyst SD-WAN Manager Release 20.18.1 or later, SD-WAN Manager does not automatically create a remote server entry.

What to do next

From Cisco Catalyst SD-WAN Manager Release 20.18.1 or later, upload the Cisco SEA application to SD-WAN Manager to connect to the Cisco SEA cloud.

Upload the Cisco SEA application to Cisco SD-WAN Manager

You can host a Cisco SEA application in one of the two ways:

- Upload the Cisco SEA application to the SD-WAN Manager local repository, or
- Upload the Cisco SEA application to a remote repository.

Before you begin

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1 and later

Download the Cisco SEA application image.

Download the ARM image file for the Cisco SEA application. Note that the **App type** should be **seaAgent**.

Procedure

Step 1 **Method 1**: If you choose to host the SEA Agent image in the SD-WAN Manager local repository, follow these steps.

This option is available in a single-tenant environment, or for a service provider operating a multitenant environment.

a) From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository**.
b) Click **Virtual Images**.
c) Click **Add New Virtual Image** and select **Manager**.
d) Choose the SEA image that you have downloaded and click **Upload**.

SD-WAN Manager creates an entry in **Virtual Images** for the locally hosted SEA image.

Step 2 **Method 2**: If you choose to host the SEA Agent image on a remote repository server, follow these steps.

This option is available in a single-tenant environment, or for tenants in a multitenant environment. Tenants in a multitenant environment can use this option if the SEA Agent image is not available in the local SD-WAN Manager repository.

a) Set up a file server and register it in SD-WAN Manager, as described in Register Remote Server.
b) From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository** > **Virtual Images**.
c) Click **Add New Virtual Image** and select **Remote Server**.
d) Enter the SEA image file name.
e) For **Select service type**, choose **App-Hosting**.
f) For **Select app type**, choose **SEA-Enterprise-Agent**.
g) Enter the version of the downloaded app.

You can see the software version on the software download page and in the package.yaml that is extracted from the SEA Agent image file (a tar file).

h) For **Select architecture**, choose **aarch64**.
i) In the **Remote Server** section, select the name of the remote server that you have registered.

The **Remote Server Details** shows the details of the locally hosted server.

j) Click **Save**.

SD-WAN Manager creates an entry in **Virtual Images** for the remotely hosted SEA Agent image.

Create a Configuration Group Profile with an SEA Feature

Before you begin

On the **Configuration** > **Configuration Groups** page, choose either

- **SD-WAN**, or
- **SD-Routing**

as the solution type.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure an SEA feature in an Other profile.

a. Enter a name and description for the feature.

Table 10: Name and Description

Field	Description
Name	Name for the feature.
Description	Optionally, add a description.

b. Configure the connection between the Cisco SEA agent and the physical interface of the host device, using virtual port group (VPG) 7. This is necessary to enable the Cisco SEA agent to reach the Cisco SEA cloud portal.

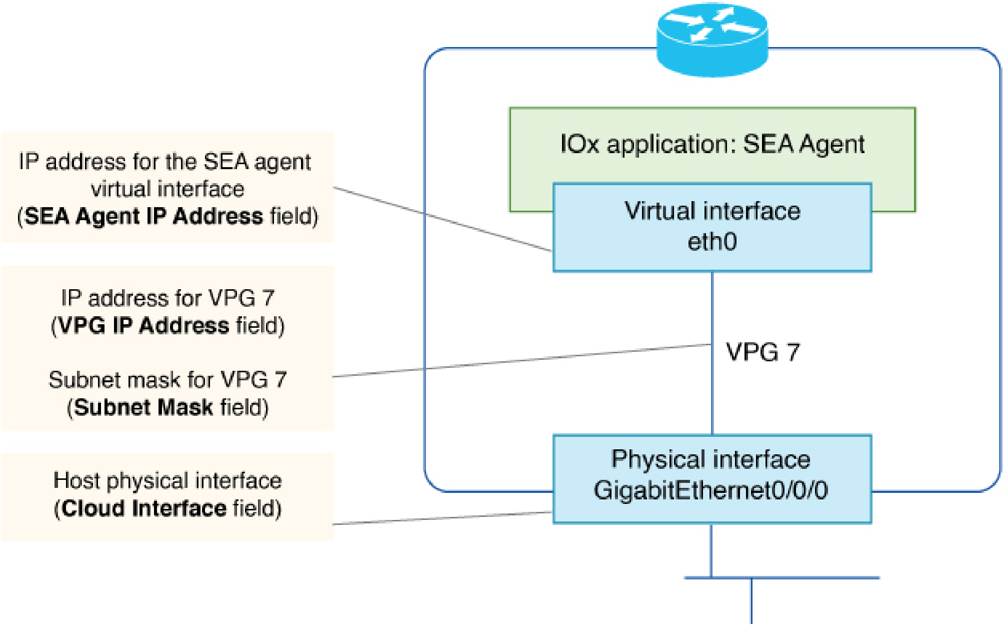

IP address for the SEA agent virtual interface (**SEA Agent IP Address** field)
IP address for VPG 7 (**VPG IP Address** field)
Subnet mask for VPG 7 (**Subnet Mask** field)
Host physical interface (**Cloud Interface** field)
IOx application: SEA Agent
Virtual interface eth0
VPG 7
Physical interface GigabitEthernet0/0/0

Table 11: Base Configuration

Field	Description
VPG IP Address	IP address to assign to virtual port group (VPG) 7. This VPG is a virtual link between the Cisco SEA agent and a physical interface of the host device. Example: 10.100.1.1

Field	Description
Subnet Mask	Subnet mask for VPG interface 7, which connects to the Cisco SEA cloud portal. Together with **VPG IP Address**, this defines the address space for the VPG 7 network. Example: 255.255.252.0
SEA Agent IP Address	IP address to assign to the Cisco SEA cloud agent to map it to VPG 7. Enter an address within the address space defined by **VPG IP Address** and **Subnet Mask**. Example: 10.100.1.2
Cloud Interface	This field appears when configuring an SEA feature for use with the SD-Routing solution. Enter the physical interface that the device uses to connect to the Cisco SEA cloud portal. The interface type can include cellular. Example: GigabitEthernet0/0/0 Example: Cellular0/1/0 **Note** For a device that you are configuring for the SD-WAN solution (not the SD-Routing solution), the VPG automatically connects to the host interface used for the control connection between the host device and Cisco SD-WAN Manager.

c. Optionally, configure one or more asset networks for connectivity to assets.

Table 12: Asset Access Networks (optional)

Field	Description
Add Access Network	Configure connectivity for up to three asset networks, each of which can include more than one asset.
Service VPN	(This field appears when configuring an SEA feature for use with the SD-WAN solution.) If your assets are distributed across multiple different service VPNs, you may need to add each of the service VPNs here. **Note** Configure route leaking to provide connectivity between (a) the service VPN used for connectivity with the Cisco SEA cloud portal, and (b) each service VPN that you configure here.
Asset Interface	(This field appears when configuring an SEA feature for use with the SD-Routing solution.) Physical interface that the device is using to connect to the asset network.
VPG IP Address	IP address to assign to the VPG interface on the router.

Field	Description
SEA Agent IP Address	IP address to assign to the SEA asset agent for mapping to the respective VPG interface on the router. The address must be within the same network as the asset VPG interface.
Subnet Mask	VPG subnet mask.
Action	A delete option removes a row of the table, removing an asset network configuration.

d. Configure a DNS server within your network, capable of resolving Cisco SEA portal domain names.

Table 13: Name Servers

Field	Description
Add Name Server	Configure a DNS server within your network, capable of resolving Cisco SEA portal domain names. Click **Add Name Server** to add a name server. For information about the Cisco SEA portal domain names, see Network ports and protocols. This is a mandatory field. If you do not configure a name server, you cannot save the configuration. Maximum number of name servers: 5
Name Server	IP address of a domain name server.
Action	A delete option removes a row of the table, removing a name server.

What to do next

Also see Deploy a configuration group.

Add a Cisco SEA Feature to a Configuration Group

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 In the solution drop-down list, choose either

- **SD-WAN**, or
- **SD-Routing**

as the solution type to display configuration groups only for this solution.

Step 3 Click the **Configuration Groups** tab.

Step 4 If you need to create a configuration group, follow the steps described in Using Configuration Groups in *Cisco Catalyst SD-WAN Configuration Groups*.

Step 5 For an existing configuration group, click **Add Profile** and add an **Other Profile** to the configuration group.

Step 6 In the configuration group, locate the **Other Profile** drop-down list and choose a Cisco SEA profile.

Deploy a Configuration Group with a Cisco SEA Feature

Before you begin

- See Supported platforms for Cisco Secure Equipment Access integration, on page 21 before deploying a configuration group with the Cisco SEA feature.
- For each device that will be running the Cisco SEA agent, ensure that device has network reachability to the Cisco SEA cloud portal before deploying a configuration group that includes the Cisco SEA feature. This requires two steps:

  1. Deploy a configuration group to establish reachability to a Cisco SEA cloud portal.
  2. Deploy a configuration group to enable Cisco SEA on the devices.

     After you confirm reachability in the previous step, you can modify the same configuration group that you used in that step, adding the Cisco SEA feature, and deploy the configuration group to the devices.

  See Prerequisites for Cisco Secure Equipment Access integration, on page 21.

Note This same requirement applies when you add devices to a configuration group that has the Cisco SEA feature and that you have deployed to devices already. If you want to deploy the configuration group to additional devices, make note of the above and first establish reachability to the Cisco SEA cloud portal for the additional devices.

Procedure

Step 1 Use the standard configuration group deployment procedure in *Cisco Catalyst SD-WAN Configuration Groups* to deploy a configuration group to devices in the network.

Step 2 If you are deploying to devices of the SD-WAN solution type, during deployment, enter any device-specific variables, as required, for each router.

If you are deploying to devices of the SD-Routing solution type, skip this step.

Step 3 If you want to monitor the progress of installing the Cisco SEA application on a device, view the log messages for the installation.

a. Click the task list button near the top right.

b. Click the **Deploy configuration group** task.

   This opens a page showing the deployment progress for each device.

c. Adjacent to a device, click the log icon in the **Action** column.

   The **View Logs** pane opens, showing the deployment progress for the device. When the deployment is complete, and when the devices have established a connection to the Cisco SEA cloud portal, a success message, such as "Config Group successfully deployed to device," appears in the log.

   When you first deploy a configuration group with the Cisco SEA feature to a device, it triggers the device to install the Cisco SEA application. It takes several minutes for a device to install the Cisco SEA application. After a successful installation, the device operates as part of the Cisco SEA solution.

Verify that Cisco SD-WAN Manager has connected to the Cisco Secure Equipment Access cloud portal

When you create a configuration group with a Cisco SEA feature, deploying the configuration group to devices triggers the devices to install the Cisco SEA application. It takes several minutes for a device to install the Cisco SEA application. After a successful installation, the device operates as part of the Cisco SEA solution.

Before you begin

Deploy a configuration group with a Cisco SEA feature to one or more devices. See Deploy a Configuration Group with a Cisco SEA Feature, on page 30.

Procedure

Step 1 Log in to the Cisco SEA cloud portal.

Step 2 View the device list. For details, see the Cisco Secure Equipment Access documentation on the Cisco DevNet site.

Verify that the Cisco Secure Equipment Access application is operating on a device, using the CLI

This verification method is applicable to devices in the SD-WAN or SD-Routing solutions.

Before you begin

Deploy a configuration group with a Cisco Secure Equipment Access feature to one or more devices. See Deploy a Configuration Group with a Cisco SEA Feature, on page 30.

Procedure

Step 1 On a device running the Cisco Secure Equipment Access application, run this command.

```
Device# show iox-service
```

Step 2 Based on the output of the command in the previous step, do one of these:

- If the command output shows that the IOxman service is running, then proceed to the next step.
- If the command output shows that the IOxman service is not running, this indicates that the Cisco Secure Equipment Access application is not operating correctly. Reinstall the application. See Deploy a Configuration Group with a Cisco SEA Feature, on page 30.

Step 3 On the same device, run this command. If the output shows that state as running, this indicates that the Cisco Secure Equipment Access application is operating correctly.

```
Device# show app-hosting detail appid sea
```

Example

In this example, the Cisco Secure Equipment Access application is installed and operating. Note that the command output is abbreviated here.

```
Device# show iox-service
IOx Infrastructure Summary:
IOx service (CAF)              : Running
IOx service (HA)               : Not Supported
IOx service (IOxman)           : Running
IOx service (Sec storage)      : Running
Libvirtd 5.5.0                 : Running
Dockerd v19.03.13-ce           : Running

Device# show app-hosting detail appid sea
App id                 : sea
Owner                  : iox
State                  : RUNNING
...
```

Monitor the Cisco Secure Equipment Access application on devices

Before you begin

Deploy a configuration group with a Cisco Secure Equipment Access feature to one or more devices. See Deploy a Configuration Group with a Cisco SEA Feature, on page 30.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

Step 2 Click a device name for a device in the SD-WAN solution.

Note

This monitoring method is applicable to devices in the SD-WAN solution, but not to devices in the SD-Routing solution.

Step 3 Click the **Real Time** tab.

Step 4 Enter any of these App Hosting commands in the **Device Options** field to view the resource usage or other details of the Cisco Secure Equipment Access application operating on the device:

- App Hosting Details
- App Hosting Utilization
- App Hosting Network Utilization
- App Hosting Storage Utilization
- App Hosting Processes
- App Hosting Attached Devices
- App Hosting Network Interfaces
- App Hosting Guest routes

CHAPTER 5

Third-Party Custom Application Integration with Cisco Catalyst SD-WAN

Third-party custom application integration with Cisco Catalyst SD-WAN

Table 14: Feature history

Feature name	Release information	Feature description
Third-party custom application integration	Cisco IOS XE Catalyst SD-WAN Release 17.16.1a Cisco Catalyst SD-WAN Manager Release 20.16.1	Cisco SD-WAN Manager supports integration with third-party-developed Cisco IOx applications. These custom applications add functionality to devices that run Cisco IOS XE Catalyst SD-WAN software.

Information about third-party custom application integration with Cisco Catalyst SD-WAN

Cisco SD-WAN Manager supports integration with third-party-developed Cisco IOx applications. These are called custom applications, and add functionality to devices that run Cisco IOS XE Catalyst SD-WAN software.

Connectivity

A Cisco IOx application operates on a device, in a Docker container. The application may or may not include connectivity to other data sources and components, such as these:

- Serial ports on the device

  See the serial port configuration in Create a Configuration Group Profile with a Custom Application Feature, on page 40.

- An application server

  See the network configuration parameters in Create a Configuration Group Profile with a Custom Application Feature, on page 40.

Virtual port group interfaces

If the third-party-developed custom application has a networking requirement, Cisco SD-WAN Manager uses virtual port group (VPG) interfaces in the range of 11 to 22, based on their availability. There is no need to reserve specific VPG interfaces.

Supported platforms for third-party custom application integration

Table 15: Supported platforms

Platform series	Models	Supported from
Cisco Catalyst IR1100 Rugged Series Routers	Cisco Catalyst IR1101	Cisco IOS XE Catalyst SD-WAN Release 17.16.1a Cisco Catalyst SD-WAN Control Components Release 20.16.1
Cisco Catalyst IR1800 Rugged Series Routers	Cisco Catalyst IR1821 Cisco Catalyst IR1831 Cisco Catalyst IR1833 Cisco Catalyst IR1835	Cisco IOS XE Catalyst SD-WAN Release 17.16.1a Cisco Catalyst SD-WAN Control Components Release 20.16.1

Prerequisites for third-party custom application integration

Resource requirements

Ensure that each device has the CPU, memory, and storage resources required for the third-party-developed custom application. The resource requirements depend entirely on the details of the custom application.

Restrictions for third-party custom application integration

Upgrade limitation

Cisco SD-WAN Manager does not support upgrading a custom application. To upgrade to a newer version, uninstall the current version and install the new version of the application. See Uninstall a third-party custom application, on page 45.

Application restart

Cisco SD-WAN Manager does not support restarting the third-party-developed custom application.

API key

The API key used for establishing a secure link with the third-party custom application has an expiration period of one year.

Multitenancy

- In Cisco Catalyst SD-WAN Manager Release 20.16.x, multitenant environments do not support integration with third-party custom applications.
- From Cisco Catalyst SD-WAN Manager Release 20.18.1, multitenant environments support integration with Cisco Secure Equipment Access only at the tenant level, not at the provider level.

Configuration group

If a third-party custom application is attached to any configuration group, the **Export** and **Import** functionalities will not work.

Configure third-party custom application integration, high level

Procedure

Step 1 Activate Cisco IOx on devices, on page 38

Step 2 Upload the third-party custom application to Cisco SD-WAN Manager, on page 38

Step 3 Create a Configuration Group Profile with a Custom Application Feature, on page 40

Step 4 Add a Custom Application Feature to a Configuration Group, on page 43

Step 5 Deploy a Configuration Group with a Custom Application Feature, on page 43

What to do next

After the configuration steps, you can monitor the activity of the application operating on a device. See Monitor a third-party custom application on devices, on page 45.

Activate Cisco IOx on devices

This procedure activates Cisco IOx on devices, which is necessary for running third-party custom Cisco IOx applications.

Before you begin

- For Cisco Catalyst SD-WAN Manager Release 20.16.x, ensure to activate Cisco IOx on devices before running third-party custom Cisco IOx applications on the devices.
- From Cisco Catalyst SD-WAN Manager Release 20.18.1, activating Cisco IOx on devices is not required.

Procedure

Step 1 Create a configuration group with a CLI add-on profile.

Step 2 In the CLI add-on profile, include the **iox** command to activate Cisco IOx.

```
iox
```

Step 3 Use the standard configuration group deployment procedure in *Cisco Catalyst SD-WAN Configuration Groups* to deploy the configuration group to devices before installing a third-party custom Cisco IOx application.

Upload the third-party custom application to Cisco SD-WAN Manager

You can host a third-party custom application in one of the two ways:

- Upload the third-party custom application to the SD-WAN Manager local repository, or
- Upload the third-party custom application to a remote repository

Before you begin

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1 and later

Custom application package

Ensure that the third-party custom application package meets the requirements described in the Cisco IOx documentation.

In addition to the above package requirements for a third-party application, ensure the image_properties.xml file uses this format:

```
<image_properties>
<vnf_type>app-hosting</vnf_type>
<name>Custom-App</name>
<arch>aarch64/x86_64</arch>
<version>0.85</version>
<imageType>dockertype</imageType>
<applicationDescription><Custom App Description></applicationDescription>
<applicationVendor>Cisco Systems</applicationVendor>
<applicationMaxInstances>1</applicationMaxInstances>
</image_properties>
```

Table 16: image_properties.xml element descriptions

Elements	Description
vnf_type	Specifies the VM functionality. It is always `app-hosting` when uploading the application image to SD-WAN Manager.
name	Name of the application. For third-party applications, use `Custom-App`.
arch	Architecture type of the third-party application. Possible values: • x86_64 • aarch64 See the package.yml file to find the application's architecture.
version	Version of the third-party application as defined in the package.yml file.
imageType	Specifies the type of image: dockertype
applicationDescription	Description of the application, as defined in the package.yml file.
applicationVendor	Name of the application vendor.
applicationMaxInstances	Maximum number of application instances.

Procedure

Step 1 **Method 1**: If you choose to host the the third-party custom application image in the SD-WAN Manager local repository, follow these steps.

This option is available in a single-tenant environment, or for a service provider operating a multitenant environment.

a) From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository**.
b) Click **Virtual Images**.
c) Click **Add New Virtual Image** and select **Manager**.
d) Choose your custom application image and click **Upload**.

SD-WAN Manager creates an entry in **Virtual Images** for the locally hosted third-party custom application.

Step 2 **Method 2**: If you choose to host the third-party custom application on a remote repository server, follow these steps.

This option is available in a single-tenant environment, or for tenants in a multitenant environment. Tenants in a multitenant environment can use this option if the custom application image is not available in the local SD-WAN Manager repository.

a) Set up a file server and register it in SD-WAN Manager, as described in Register Remote Server.
b) From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository** > **Virtual Images**.

c) Click **Add New Virtual Image** and select **Remote Server**.
d) Enter the third-party custom application image file name.
e) For **Select service type**, choose **App-Hosting**.
f) For **Select app type**, choose **Custom-App**.
g) Enter the version of your custom application.
h) For **Select architecture**, choose **aarch64** or **x86_64**.
i) In the **Remote Server** section, select the name of the remote server that you have registered.

   The **Remote Server Details** shows the details of the locally hosted server.

j) Click **Save**.

SD-WAN Manager creates an entry in **Virtual Images** for the remotely hosted third-party custom application.

Create a Configuration Group Profile with a Custom Application Feature

Because third-party-developed custom applications are unique, Cisco SD-WAN Manager cannot validate the configuration against a common standard. To ensure that the application operates correctly, configure the parameters here according to the requirements of the application.

Before you begin

On the **Configuration** > **Configuration Groups** page, choose either

- **SD-WAN**, or
- **SD-Routing**

as the solution type.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure a Custom Application feature in an Other profile.

a. Enter a name and description for the feature.

Table 17: Name and Description

Field	Description
Name	Name for the feature.
Description	Optionally, add a description.

b. The basic settings are mandatory.

Table 18: Basic Settings

Field	Description
Application Name	Enter a name for the custom application. You can use upper- or lower-case letters, but not spaces or special characters. This name appears as part of the event details on the **Monitor** > **Logs** > **Events** page.
Virtual Image	Choose a custom application image file from the drop-down list. The list shows custom application images uploaded to the virtual image repository in **Maintenance** > **Software Repository** > **Virtual Images**.

c. If the custom application has a requirement for network configuration, click **Add Configuration** and enter the network connectivity details for up to three connections. This configures communication between the Cisco IOx application and

- the device on which the application is operating, and
- any external assets, such as a server if the application communicates with a server.

Note
At least one network configuration is required for a third-party custom application.

Here are the options for the SD-WAN solution:

Table 19: Network Configuration, SD-WAN Solution

Field	Description
Name	Name describing the entity for which you are configuring connectivity.
Service VPN	Service VPN providing the connectivity between the application and either (a) the device, or (b) an external asset.
VPG IP Address	IP address within the subnet mask defined in the **Subnet Mask** field for communication between the custom application and a device virtual port group (VPG) interface or external asset.
Application IP Address	IP address to assign to the custom application, for mapping to a VPG interface on the device.
Subnet Mask	Subnet mask for the VPG interface. The subnet mask defines an address space for the service VPN for communication between the custom application and a device VPG interface or external asset.
Action	Provides an option to delete a row.

Here are the options for the SD-Routing solution:

Table 20: Network Configuration, SD-Routing Solution

Field	Description
Network Configuration	
Name	Name describing the entity for which you are configuring connectivity.
Communication Interface	Physical or virtual interface providing connectivity between the application and either (a) the device, or (b) an external asset.
Action	Provides an option to delete a row.

d. Some custom applications require information passed as variables, either global or device-specific. To add variables, click **Add Variable** and enter the details.

The specifics of the valid key:value pairs depend entirely on the details of the custom application. Consult with the custom application developer for information about configuring variables. Note that these values are case sensitive.

Maximum number of variables: 10

Table 21: Environment Variables

Field	Description
Key	Key name for a variable.
Value	Value of the variable. Choose **Device Specific** to provide a specific key value for each device.
Action	Provides an option to delete a row.

e. Some custom applications use data input provided through a serial interface. This option supports any serial port available on the platform.

To add a data source, click **Add Data Source** and enter the serial port.

Maximum number of serial ports: 7

Table 22: Data Configuration

Field	Description
Serial Line	Enter a serial port available on the device. See the platform documentation for information about serial ports. Example: /dev/ttySerial
Action	Provides an option to delete a row.

What to do next

Also see Deploy a configuration group.

Add a Custom Application Feature to a Configuration Group

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 In the solution drop-down list, choose either

- **SD-WAN**, or
- **SD-Routing**

as the solution type to display configuration groups only for this solution.

Step 3 Click the **Configuration Groups** tab.

Step 4 If you need to create a configuration group, follow the steps described in Using Configuration Groups in *Cisco Catalyst SD-WAN Configuration Groups*.

Step 5 For an existing configuration group, click **Add Profile** and add an **Other Profile** to the configuration group.

Step 6 In the configuration group, locate the **Other Profile** drop-down list and choose a Custom Application profile.

Deploy a Configuration Group with a Custom Application Feature

Before you begin

See Supported platforms for third-party custom application integration, on page 36 before deploying a configuration group with the Custom Application feature.

Activate Cisco IOx on devices before deploying the configuration group. See Activate Cisco IOx on devices, on page 38.

Procedure

Step 1 Use the standard configuration group deployment procedure in *Cisco Catalyst SD-WAN Configuration Groups* to deploy a configuration group to devices in the network.

Step 2 If you are deploying to devices of the SD-WAN solution type, during deployment, enter any required device-specific variables for each router.

Step 3 If you want to monitor the progress of installing the application on a device, view the log messages for the installation.

a. Click the task list button near the top right.

b. Click the **Deploy configuration group** task.

This opens a page showing the deployment progress for each device.

c. Adjacent to a device, click the log icon in the **Action** column.

The **View Logs** pane opens, showing the deployment progress for the device. When the deployment is complete, a success message, such as "Config Group successfully deployed to device," appears in the log.

When you first deploy a configuration group with the Custom Application feature to a device, it triggers the device to install the application.

Verify that a third-party custom application is operating on a device, using the CLI

This verification method is applicable to devices in the SD-WAN or SD-Routing solutions.

Before you begin

Deploy a configuration group with a Custom Application feature to one or more devices. See Deploy a Configuration Group with a Custom Application Feature, on page 43.

Procedure

Step 1 On a device running the Cisco IOx application, run this command.

```
Device# show iox-service
```

Step 2 Based on the output of the command in the previous step, do one of these:

- If the command output shows that the IOxman service is running, then proceed to the next step.
- If the command output shows that the IOxman service is not running, this indicates that the Cisco IOx application is not operating correctly. Reinstall the application. See Deploy a Configuration Group with a Custom Application Feature, on page 43.

Step 3 On the same device, run this command. If the output shows the state as running for the application you are checking, this indicates that the application is operating correctly.

```
Device# show app-hosting detail appid application-id
```

Example

The application name that you enter in the Custom Application feature determines the application ID that appears in the command output. See Create a Configuration Group Profile with a Custom Application Feature, on page 40. In this example, the application ID is abc.

The command output is truncated here.

```
Device# show iox-service
IOx Infrastructure Summary:
IOx service (CAF)              : Running
IOx service (HA)               : Not Supported
IOx service (IOxman)           : Running
IOx service (Sec storage)      : Running
Libvirtd 5.5.0                 : Running
```

```
Dockerd v19.03.13-ce           : Running

Device# show app-hosting detail appid abc
App id                 : abc
Owner                  : iox
State                  : RUNNING
...
```

Monitor a third-party custom application on devices

Before you begin

Deploy a configuration group with a Custom Application feature to one or more devices. See Deploy a Configuration Group with a Custom Application Feature, on page 43.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

Step 2 Click a device name for a device in the SD-WAN solution.

Note
This monitoring method is applicable to devices in the SD-WAN solution, but not to devices in the SD-Routing solution.

Step 3 Click the **Real Time** tab.

Step 4 Enter any of these App Hosting commands in the **Device Options** field to view the resource usage or other details of applications operating on the device, including a third-party-developed custom applications:

- App Hosting Details
- App Hosting Utilization
- App Hosting Network Utilization
- App Hosting Storage Utilization
- App Hosting Processes
- App Hosting Attached Devices
- App Hosting Network Interfaces
- App Hosting Guest routes

Uninstall a third-party custom application

Uninstalling a third-party-developed custom application presumes that you have installed the application already. See Configure third-party custom application integration, high level, on page 37.

Procedure

Step 1 Remove the Custom Application feature from the configuration group.

a) From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
b) Click the **Configuration Groups** tab.
c) Adjacent to a configuration group, click the arrow in the **Actions** column to expand the row to show the attached profiles.
d) Adjacent to the **Other Profile** drop-down list, click the pencil icon to edit the profile.
e) Within the profile, remove the Custom Application feature.

Step 2 Deploy the configuration group to devices. See Deploy a Configuration Group with a Custom Application Feature, on page 43.

The procedure uninstalls the custom application from devices to which it had been deployed.