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 traffic on one or more interfaces and send the 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 sensors, to use Cisco Cyber Vision terminology. A sensor is a device, such as a router, that you configure to monitor traffic on one or more interfaces and send the traffic to Cisco Cyber Vision Center to analyze for security concerns. These sensors are an integral part of what enables Cisco Cyber Vision to manage security threats in the network.

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.

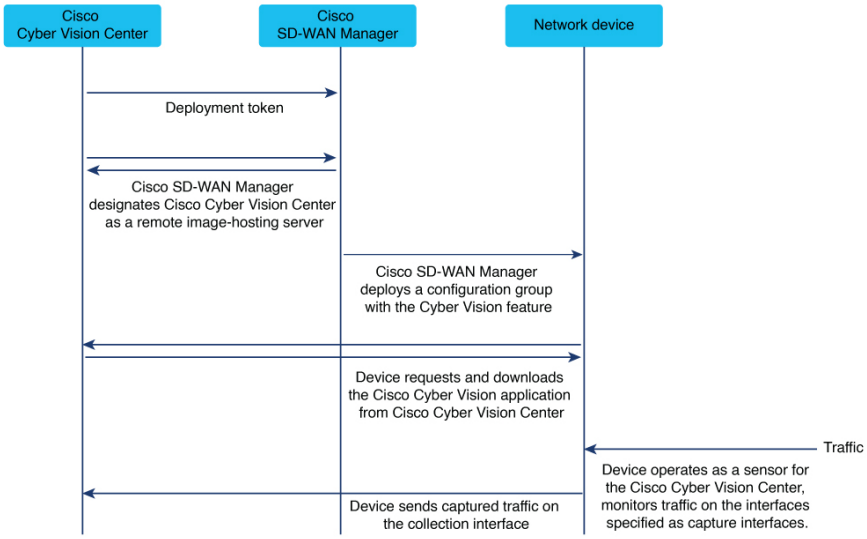
After a successful installation, the device operates as a sensor for Cisco Cyber Vision. The device appears in the sensor list in Cisco Cyber Vision Center.

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



1. As described in the Configure a Connection to a Cisco Cyber Vision Center in the Network Hierarchy, on page 5 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 5 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 4, 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

Cisco Catalyst IR1101 Rugged Series

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 Cisco Catalyst IR1101 Rugged Series platform is running the Cisco Cyber Vision application, the device cannot run other Cisco IOx applications.

Configure Cisco Cyber Vision Integration, High Level

Step 1 Configure a Connection to a Cisco Cyber Vision Center in the Network Hierarchy, on page 5
Step 2 Create a Configuration Group Profile with a Cyber Vision Feature, on page 6
Step 3 Add a Cyber Vision Feature to a Configuration Group, on page 8
Step 4 Deploy a Configuration Group with a Cisco Cyber Vision Feature, on page 8

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 11.

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 2: 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.

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 2.

Create a Configuration Group Profile with a Cyber Vision Feature

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 for the configuration group.

Step 3 Click the **Other Profile** tab.

Step 4 Click **Add New**.

Step 5 In the **Add Feature Profile** pop-up window, enter a name and description for the profile, and click **Create**.

Step 6 Click **Add New Feature** and choose **Cyber Vision**.

Step 7 Enter the parameters for your Cyber Vision Center server.

Field	Description
Name	Name for the Cisco Cyber Vision Center.
Description	Optionally, add a description.

Field	Description
Base Configuration area	
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, on page 5.
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

Field	Description
Advanced Configuration area This 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 8. But you can configure global device values instead of using the variables.	
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, seeConfigure a Connection to a Cisco Cyber Vision Center in the Network Hierarchy, on page 5.
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.
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.

Field	Description
VPG6 (Virtual Port Group) IP Address	This field is preset and not configurable.

Add a Cyber Vision Feature to a Configuration Group

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 4 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 4.

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.

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 5.
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 10.

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 8.

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 8.

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 8.

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 8.

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