Cisco Catalyst SD-WAN Solution Integrations Guide, Releases 26.x and Later

Cisco SD-WAN
Updated September 28, 2026

© 2026 Cisco Systems, Inc. All rights reserved.

Full Cisco Trademarks with Software License

Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

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

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Topics included

Full Cisco Trademarks with Software License....ii

1 Cisco Cyber Vision Integration with Cisco Catalyst SD-WAN....7

Feature history for Cisco Cyber Vision integration with Cisco Catalyst SD-WAN....8
Cisco cyber vision integration....8
Cisco cyber vision application....9
How the Cisco Cyber Vision application works....9
Use Cisco Cyber Vision Center....10
Supported platforms for Cisco cyber vision integration....11
Prerequisites for Cisco cyber vision integration....11
Restrictions for Cisco cyber vision integration....12
Configure Cisco cyber vision integration....12
Configure a Cyber Vision Center connection....13
Create a configuration group profile with a cyber vision feature....14
Add a cyber vision feature to a configuration group....17
Deploy a configuration group with a Cisco cyber vision feature....17
Verify Cisco Cyber Vision Integration....19
Verify SD-WAN Manager connection....19
Verify Cisco cyber vision application using the CLI....20
Monitor the Cisco cyber vision application on devices....21

2 Cisco Secure Equipment Access integration with Cisco Catalyst SD-WAN....23

Feature history for Cisco Secure Equipment Access integration with Cisco Catalyst SD-WAN....24
Cisco secure equipment access integration....24
Benefits of Cisco secure equipment access integration....25
Cisco secure equipment access application....25
Cisco secure equipment access solution....25
Supported platforms for Cisco secure equipment access integration....26
Prerequisites for Cisco secure equipment access integration....26
Restrictions for Cisco secure equipment access integration....27
Configure Cisco secure equipment access integration....27
Configure a connection to a Cisco secure equipment access portal in the network hierarchy....28
Upload the Cisco SEA application to Cisco SD-WAN Manager....30
Create a configuration group profile with an SEA feature....31
Add a Cisco SEA feature to a configuration group....34
Deploy a configuration group with a Cisco SEA feature....35
Verify the Cisco Secure Equipment Access integration....36
Verify the Secure Equipment Access connection....36

Verify the Secure Equipment Access application using the CLI....37
Monitor the Cisco secure equipment access application on devices....38

3 Third-Party Custom Application Integration with Cisco Catalyst SD-WAN....39
Feature history for Third-party custom application integration with Cisco Catalyst SD-WAN....40
Third-party custom application integration with Cisco Catalyst SD-WAN....40
Supported platforms for third-party custom application integration....40
Prerequisites for third-party custom application integration....41
Restrictions for third-party custom application integration....41
Configure third-party custom application integration....42
Activate Cisco IOx on devices....42
Upload the third-party custom application to Cisco SD-WAN Manager....43
Create a configuration group profile with a custom application feature....44
Add a custom application feature to a configuration group....47
Deploy a configuration group with a custom application feature....48
Uninstall a third-party custom application....49
Verify that a third-party custom application using the CLI....49
Monitor a third-party custom application on devices....50

4 Cisco Unified Communications Voice Services....53
Feature history for Cisco unified communications voice services....54
Cisco unified communications voice services....54
Configure unified communications voice services....55
Add a voice card feature template....56
Add call routing feature template....65
Add an SRST feature template....69
Add a DSPFarm feature template....71
Add a voice policy....81
Provision a device template for unified communications....118
Generated CLI commands for subpolicies to endpoints mapping....120
Dial peer CSV file....121
Translation rules CSV file....122
Monitor UC operations....123
Voice calls monitoring information....124
Voice VoIP calls monitoring information....125
Voice phone info monitoring information....125
Voice controller T1 E1 current 15 Mins stats monitoring information....126
Voice controller T1 E1 total stats monitoring information....127
Voice ISDN status information....128
Voice DSPFarm SCCP CUCM groups monitoring information....128
Voice DSPFarm profile monitoring information....129
Voice DSPFarm SCCP connections monitoring information....130
Voice DSPFarm active monitoring information....131

5 Cisco Unified Communications FXS and FXO Caller ID.....133
Feature History for Cisco Unified Communications FXS and FXO Caller ID.....134
Cisco Unified Communications FXS and FXO Caller ID Support.....134
Supported devices for adding voice features with CLI add-on feature templates.....134
Restrictions for Adding Voice Features with a CLI Add-On Feature Template.....135
Voice-feature configuration commands for a CLI add-on Feature Template.....135

6 Cisco unified border element.....137
Feature history for Cisco unified border element.....138
Cisco unified border elements (CUBE).....139
Supported devices for CUBE configuration.....139
Restrictions for CUBE configuration.....140
Use cases for CUBE.....140
Configure CUBE.....140
CUBE commands.....142
SRST commands.....149

7 Onboarding ThousandEyes Agent and Onboarding Tests.....151
Feature History for Simplified Onboarding of Cisco ThousandEyes Agent.....152
Onboarding Cisco ThousandEyes agents and configuring tests.....152
Create an IP pool for the Cisco ThousandEyes agents.....152
Prerequisites for simplified workflow.....153
Restrictions for simplified workflow.....154
Configure Cisco ThousandEyes agent and tests using simplified workflow.....154
Monitor onboarded Cisco ThousandEyes agents and configured tests.....155
Troubleshoot Cisco ThousandEyes agent on edge device.....156

8 Monitoring with Cisco ThousandEyes.....157
Feature history for extended visibility with Cisco Catalyst SD-WAN and ThousandEyes.....158
Extending visibility for Cisco Catalyst SD-WAN and Cisco ThousandEyes.....159
Supported devices for running Cisco SD-WAN and Cisco ThousandEyes.....159
ThousandEyes enterprise agent supported versions and system requirements.....162
Prerequisites for extending visibility with SD-WAN manager and Cisco ThousandEyes.....163
Restrictions for extending visibility with SD-WAN manager and Cisco ThousandEyes.....163
Configure a Cisco ThousandEyes enterprise agent using a configuration group.....164
Upload the Cisco ThousandEyes Enterprise Agent software to SD-WAN Manager.....166
Provision Cisco ThousandEyes Enterprise Agent in a Service VPN or Transport VPN (VPN0).....167
Provision a Cisco ThousandEyes enterprise agent in a service VPN using CLI.....169
Uninstall the Cisco ThousandEyes enterprise agent software.....171
Upgrade the Cisco ThousandEyes enterprise agent software.....172
Troubleshoot the Cisco ThousandEyes Enterprise Agent on Cisco IOS XE Catalyst SD-WAN devices.....172

1 Cisco Cyber Vision Integration with Cisco Catalyst SD-WAN

Topics:

- Feature history for Cisco Cyber Vision integration with Cisco Catalyst SD-WAN
- Cisco cyber vision integration
- Cisco cyber vision application
- How the Cisco Cyber Vision application works
- Use Cisco Cyber Vision Center
- Supported platforms for Cisco cyber vision integration
- Prerequisites for Cisco cyber vision integration
- Restrictions for Cisco cyber vision integration
- Configure Cisco cyber vision integration
- Verify Cisco Cyber Vision Integration
- Monitor the Cisco cyber vision application on devices

Describes how to integrate Cisco Cyber Vision with external security platforms and management systems to enhance industrial network visibility and threat detection capabilities.

Feature history for Cisco Cyber Vision integration with Cisco Catalyst SD-WAN

Provides feature history information for Cisco Cyber Vision integration with SD-WAN solutions.

This reference provides the feature history for Cisco Cyber Vision integration with Cisco Catalyst SD-WAN. The integration enables network security monitoring and traffic analysis through Cisco SD-WAN Manager configuration.

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.

Cisco cyber vision integration

Describes the integration capabilities between Cisco Cyber Vision and Cisco Catalyst SD-WAN.

Cisco Cyber Vision integration is a network security solution that

- 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
- enables Cisco SD-WAN Manager to configure devices in the network to operate as software-based sensors.

Integration value

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.

The browser-based manager is called Cisco Cyber Vision Center. Documentation for Cisco Cyber Vision is available here.

Cisco Catalyst SD-WAN support for Cyber Vision includes

- monitoring L3 interfaces on all supported platforms, and
- monitoring L2 and L3 interfaces individually or simultaneously, on IR8340 platforms.

Configure the interfaces to monitor in a configuration group, using the Other profile and the Cyber Vision feature.

Depending on the interface types, SD-WAN Manager adds these configurations in the background:

Table 2: Interface monitoring configurations

Monitor	SD-WAN Manager adds these configurations for sending monitored traffic to Cyber Vision Center
L2 interfaces	VLAN 2340 Monitor session
L3 interfaces	Monitor session

Cisco cyber vision application

Describes the Cisco Cyber Vision application that provides additional functionality for network devices through a downloadable Cisco IOx application.

A Cisco Cyber Vision application is a Cisco IOx application that

- operates in a Docker container together with Cisco IOS XE Catalyst SD-WAN to provide additional functionality
- is downloaded and installed when you enable Cisco Cyber Vision on a device, rather than being included as part of a Cisco IOS XE Catalyst SD-WAN software release, and
- transforms the device into a sensor for Cisco Cyber Vision that appears in the sensor list in Cisco Cyber Vision Center after successful installation.

How the Cisco Cyber Vision application works

Describes how devices download and install the Cisco Cyber Vision application through integration with Cisco Cyber Vision Center as a remote image-hosting server.

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.

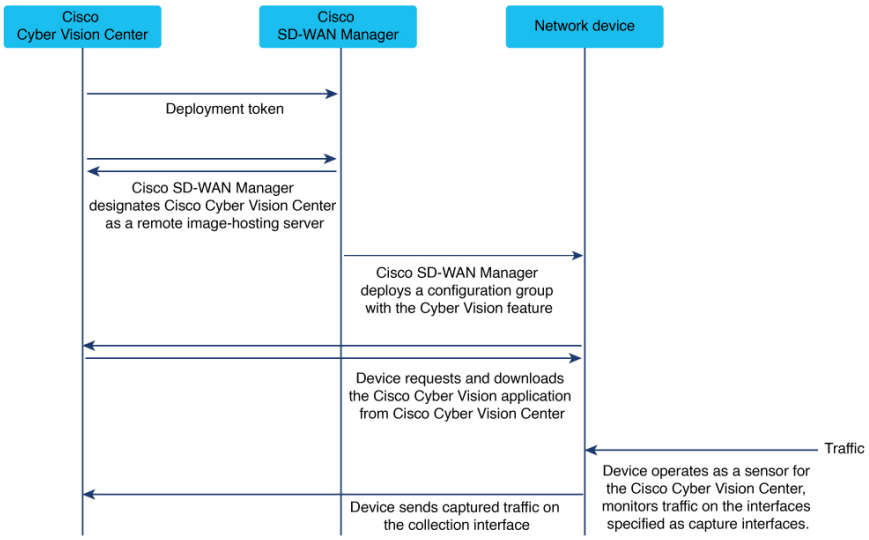
Summary

The key components involved in this process are:

- Cisco Cyber Vision Center: Serves as the remote image-hosting server and generates deployment tokens for device authentication
- Cisco SD-WAN Manager: Manages the configuration and designates Cisco Cyber Vision Center as the application host
- Network devices: Download, install, and activate the Cisco Cyber Vision application to operate as sensors
- Deployment token: Provides authentication information for devices to access Cisco Cyber Vision Center

Workflow

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



These stages describe how devices download and install the Cisco Cyber Vision application:

1. The administrator logs in to Cisco Cyber Vision Center and generates a deployment token as part of the configuration prerequisites.

   As described in the Configure a Cyber Vision Center connection on page 13 procedure prerequisites, you log in to Cisco Cyber Vision Center and generate a type of token called a deployment token.

2. Cisco SD-WAN Manager uses the deployment token information to designate Cisco Cyber Vision Center as the application host.

   When you complete the Configure a Cyber Vision Center connection on page 13 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 Caution: do not remove remote servers, do not edit or remove the server.

3. The devices connect to Cisco Cyber Vision Center to download the Cisco Cyber Vision application when a configuration is pushed to them.

   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, enabling them to operate as sensors for the Cisco Cyber Vision Center.

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

Use Cisco Cyber Vision Center

Describes using Cisco Cyber Vision Center to monitor the security of the network you are managing with Cisco Catalyst SD-WAN.

Using Cisco Cyber Vision Center is a security monitoring approach that enables devices to operate as sensors for comprehensive network security oversight when managing networks with Cisco Catalyst SD-WAN.

Implementation procedures

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

Lists the supported platforms for Cisco Cyber Vision integration.

This reference provides information about the supported platforms for Cisco Cyber Vision integration, including platform series, models, and supported release versions.

Table 3: 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
Cisco Catalyst IR8300 Rugged Series	IR8340	Cisco Catalyst SD-WAN Control Components Release 26.1.1.1

Prerequisites for Cisco cyber vision integration

Outlines the requirements that must be met before integrating Cisco Cyber Vision with your network devices.

Cisco cyber vision center version

Requirement: Use Cisco Cyber Vision Center Release 5.0.0 or later

Network reachability to Cisco cyber vision center

Requirement: 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:
- Deploy a configuration group to a set of devices to establish reachability to Cisco Cyber Vision Center first, then deploy a configuration group to enable Cisco Cyber Vision on the devices.
- After you confirm reachability, 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, first establish reachability to Cisco Cyber Vision Center for the additional devices.

Virtual port groups

Requirement: Ensure that virtual port group (VPG) interfaces 5 and 6 are available for the Cisco Cyber Vision application and are not configured for use with a different application.

Do not edit or remove remote servers that Cisco SD-WAN Manager adds as Cisco Cyber Vision Center instances on the **Maintenance** > **Software Repository** page, in the **Remote server** tab.

Restrictions for Cisco cyber vision integration

Outlines restrictions for Cisco Cyber Vision integration including application limitations, onboarding constraints, and multitenancy support requirements.

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 Cyber Vision Center connection on page 13, 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

Multitenancy support varies by software version:

- 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

Configure Cisco Cyber Vision integration through a high-level overview of the required configuration steps.

This task provides a high-level workflow to configure Cisco Cyber Vision integration with SD-WAN.

Use this high-level overview to understand the sequence of configuration steps required for Cisco Cyber Vision integration. Complete each referenced task in the specified order to ensure proper integration setup.

Procedure

1. Configure a Cyber Vision Center connection on page 13
2. Create a configuration group profile with a cyber vision feature on page 14
3. Add a cyber vision feature to a configuration group on page 17
4. Deploy a configuration group with a Cisco cyber vision feature on page 17

You have completed the high-level configuration workflow for Cisco Cyber Vision integration. The integration is now configured and ready for deployment.

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 21.

Configure a Cyber Vision Center connection

Configure a connection between your network devices and a Cisco Cyber Vision Center to enable secure communication and integration.

Establishing a connection to a Cisco Cyber Vision Center enables your network devices to communicate securely with the center for industrial network monitoring and threat detection capabilities.

Use this procedure when you need to integrate Cisco Cyber Vision Center with your network infrastructure to monitor industrial protocols and detect security threats in your operational technology environment.

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 4: 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.

Follow these steps to configure a connection to a Cisco Cyber Vision Center in the network hierarchy:

Procedure

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

2. Click **External Services**.
3. In the **Cyber Vision** pane, click **Add Cyber Vision Center**.
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.

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 the Cisco Cyber Vision application works on page 9.

The connection to the Cisco Cyber Vision Center is configured and the system automatically sets up a remote image-hosting server for software repository access.

Create a configuration group profile with a cyber vision feature

Configure a Configuration Group Profile that includes a Cyber Vision feature for SD-WAN or SD-Routing solution types.

Create a Configuration Group Profile that includes a Cyber Vision feature to enable network visibility and security monitoring capabilities across your SD-WAN or SD-Routing infrastructure.

Configuration Group Profiles with Cyber Vision features provide enhanced network monitoring and security capabilities. This configuration enables you to deploy consistent Cyber Vision settings across multiple devices in your network.

Before you begin

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

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

as the solution type.

Follow these steps to create a Configuration Group Profile with a Cyber Vision feature:

Procedure

---

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

2. Create and configure a Cyber Vision feature in an Other profile.
   a. Enter a name and description for the feature.

      Table 5: Name and Description

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

   b. Configure the base configuration fields.

      Table 6: 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. Refer to 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 17. But you can configure global device values instead of using the variables.

      Table 7: 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.

Field	Description
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.
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.

You have successfully created a Configuration Group Profile with a Cyber Vision feature that can be deployed to devices in your network.

What to do next

Also see Deploy a configuration group.

Add a cyber vision feature to a configuration group

Configure a Cyber Vision profile within an existing configuration group to enable network security monitoring capabilities.

Add a Cyber Vision feature to a configuration group to integrate network security monitoring and threat detection capabilities into your SD-WAN or SD-Routing deployment.

Cyber Vision profiles provide network visibility and security monitoring features that can be applied to configuration groups for centralized management across multiple devices in your network deployment.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
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.
3. Click the **Configuration Groups** tab.
4. If you need to create a configuration group, follow the steps described in Using Configuration Groups in *Cisco Catalyst SD-WAN Configuration Groups*.
5. For an existing configuration group, click **Add Profile** and add an **Other Profile** to the configuration group.
6. In the configuration group, locate the **Other Profile** drop-down list and choose a Cisco Cyber Vision profile.

The Cyber Vision profile is successfully added to the configuration group, enabling network security monitoring capabilities for devices associated with this configuration group.

Deploy a configuration group with a Cisco cyber vision feature

Deploy a configuration group with the Cisco Cyber Vision feature to enable devices to operate as sensors for network monitoring.

Deploy a configuration group with the Cisco Cyber Vision feature to enable devices in the network to operate as sensors that capture and send traffic data to Cisco Cyber Vision Center for network monitoring and security analysis.

Use this procedure when you need to deploy the Cisco Cyber Vision feature to devices in your SD-WAN network. The deployment enables devices to function as sensors that monitor network traffic and communicate with the Cisco Cyber Vision Center.

Before you begin

- See Supported platforms for Cisco cyber vision integration on page 11 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 11.

> **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.

Follow these steps to deploy a configuration group with the Cisco Cyber Vision feature:

Procedure

1. Use the configuration group deployment procedure in *Cisco Catalyst SD-WAN Configuration Groups Reference Guide* to deploy a configuration group to devices in the network.
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 Cyber Vision Center connection on page 13.
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.

Field	Description
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.

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 SD-WAN Manager connection on page 19.

The configuration group with the Cisco Cyber Vision feature is deployed to the selected devices. The devices install the Cisco Cyber Vision application and begin operating as sensors that capture traffic and send it to Cisco Cyber Vision Center for network monitoring and security analysis. The devices appear in the sensor list in Cisco Cyber Vision Center.

Verify Cisco Cyber Vision Integration

Outlines the steps for verifying Cisco Cyber Vision integration to ensure proper deployment and connectivity.

Verify SD-WAN Manager connection

Verify that devices with deployed Cisco Cyber Vision configuration groups appear as active sensors in the Cisco Cyber Vision Center.

Verify that the Cisco Cyber Vision application has been successfully installed on devices and that the devices are operating as sensors for Cisco Cyber Vision.

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 17.

Follow these steps to verify that Cisco SD-WAN Manager has connected to the Cisco Cyber Vision Center:

Procedure

1. Log in to the Cisco Cyber Vision Center.
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.

The devices with deployed Cisco Cyber Vision configuration groups appear as active sensors in the Cisco Cyber Vision Center sensor list.

Verify Cisco cyber vision application using the CLI

Verify that the Cisco Cyber Vision application is correctly operating on devices in SD-WAN or SD-Routing solutions using CLI commands.

Use this task to verify that the Cisco Cyber Vision application is correctly installed and operating on a device after deployment.

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 17.

Follow these steps to verify that the Cisco Cyber Vision application is operating on a device:

Procedure

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

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

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 17.

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
```

The Cisco Cyber Vision application is verified to be operating correctly when both commands show the IOxman service and the cv application state as running.

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

Configure monitoring of the Cisco Cyber Vision application to view resource usage and operational details on SD-WAN devices.

Monitor the resource usage and operational status of the Cisco Cyber Vision application deployed on SD-WAN devices to ensure optimal performance and troubleshoot issues.

This task applies to devices in the SD-WAN solution that have the Cisco Cyber Vision application deployed through a configuration group. Use this monitoring capability to track application performance and resource consumption.

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 17.

Follow these steps to monitor the Cisco Cyber Vision application on devices:

Procedure

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

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

The system displays the requested information about the Cisco Cyber Vision application, including resource usage, utilization statistics, and operational details based on the selected App Hosting command.

2 Cisco Secure Equipment Access integration with Cisco Catalyst SD-WAN

Topics:

- Feature history for Cisco Secure Equipment Access integration with Cisco Catalyst SD-WAN
- Cisco secure equipment access integration
- Cisco secure equipment access application
- Cisco secure equipment access solution
- Supported platforms for Cisco secure equipment access integration
- Prerequisites for Cisco secure equipment access integration
- Restrictions for Cisco secure equipment access integration
- Configure Cisco secure equipment access integration
- Verify the Cisco Secure Equipment Access integration
- Monitor the Cisco secure equipment access application on devices

Describes how to integrate Cisco Secure Equipment Access with external systems and platforms to enhance network security and access control capabilities.

Feature history for Cisco Secure Equipment Access integration with Cisco Catalyst SD-WAN

Provides information about Cisco Secure Equipment Access integration with Cisco Catalyst SD-WAN.

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.

Table 8: 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.

Cisco secure equipment access integration

Describes the integration between Cisco Secure Equipment Access and Cisco Catalyst SD-WAN for remote access management.

Cisco Secure Equipment Access integration is a solution that

- provides remote access to network-connected assets through integration with Cisco Catalyst SD-WAN
- enables management of SEA agents on overlay network devices using Cisco SD-WAN Manager, and
- configures connectivity between overlay network devices and the Cisco Secure Equipment Access cloud portal.

SEA integration capabilities

Integration with Cisco Catalyst SD-WAN enables you to use Cisco SD-WAN Manager to perform these tasks:

- 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.

Assets can include anything reachable by IP address, such as servers, industrial internet of things (IIoT) devices, and so on. 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

Describes the benefits of Cisco Secure Equipment Access integration with Cisco Catalyst SD-WAN.

Cisco Secure Equipment Access (SEA) integration is a Zero-Trust Network Access (ZTNA) solution that

- enables remote access to operational technology (OT) assets without time-consuming and costly site visits
- operates through existing routers and switches with no dedicated hardware to install and manage, and
- provides comprehensive security capabilities with advanced cybersecurity controls and easy-to-build policies based on identities and contexts.

Key benefits

Cisco SEA provides these 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

Describes the Cisco IOx application that provides Cisco SEA functionality to network devices and enables communication with the Cisco SEA cloud portal.

A Cisco Secure Equipment Access application is a Cisco IOx application that

- provides Cisco SEA functionality to a device (a router in the network)
- downloads and installs automatically when you enable Cisco SEA on a device through Cisco SD-WAN Manager, and
- enables communication with the Cisco SEA cloud portal after successful installation.

Installing the SEA agent

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.

Cisco secure equipment access solution

Describes an integrated solution that enables devices to operate as part of a secure equipment access management system.

A Cisco Secure Equipment Access solution is an integrated security system that enables devices to operate as part of a managed access control environment for remote assets.

Additional information

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

Lists supported platforms for Cisco SEA integration.

This reference provides information about the supported platforms for Cisco Secure Equipment Access integration.

Table 9: 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

Outlines prerequisites for Cisco Secure Equipment Access integration with Cisco Catalyst SD-WAN.

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.

- Deploy a configuration group to a set of devices to establish reachability to a Cisco SEA cloud portal.
- Deploy 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 27.

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

Outlines limitations and constraints when integrating Cisco Secure Equipment Access with Cisco SD-WAN Manager.

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:

- From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository** > **Remote server**.
- Edit the remote server for SEA to use the locally hosted remote server that you have configured. Edit the automatically created server, called: SEA-RemoteServer and 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

Multitenant environment support varies by version:

- 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

Configure Cisco Secure Equipment Access integration with this high level overview of the required steps.

This task provides a high level overview of the steps required to integrate Cisco Secure Equipment Access with your SD-WAN deployment.

Use this workflow when you need to set up Cisco Secure Equipment Access integration from start to finish. Complete each step in the specified order to ensure proper configuration.

Procedure

1. Configure a connection to a Cisco secure equipment access portal in the network hierarchy on page 28
2. Upload the Cisco SEA application to Cisco SD-WAN Manager on page 30
3. Create a configuration group profile with an SEA feature on page 31
4. Add a Cisco SEA feature to a configuration group on page 34
5. Deploy a configuration group with a Cisco SEA feature on page 35

You have completed the high level configuration steps for Cisco Secure Equipment Access integration.

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 38.

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.

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.

This configuration enables devices to establish a secure link with the Cisco SEA cloud portal for enhanced security and access management.

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. Refer to the Register Remote Server section of the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide* for setup instructions.

Follow these steps to configure a connection to a Cisco Secure Equipment Access portal in the Network Hierarchy:

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy**.
2. Click **External Services**.
3. In the **Secure Equipment Access Cloud** pane, enter these:

Table 10: 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. **Note** Starting from SD-WAN Manager 26.1.1.1, you can edit the Secure Equipment Access (SEA) API key in the Secure Equipment Access Cloud window for external services. Updating the API key does not require stopping any running configurations. You must re-deploy the configuration groups after updating the SEA API key.
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 27.
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 27.

4. Click **Save**.

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.

A secure connection is established between your network devices and the Cisco Secure Equipment Access cloud portal through the Network Hierarchy configuration.

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

Configure the Cisco SEA application upload to Cisco SD-WAN Manager using either local repository or remote server hosting methods.

This task enables you to host a Cisco SEA application in SD-WAN Manager for deployment across your network infrastructure.

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

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.

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. Refer to the Register Remote Server section of the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide* for setup instructions.
   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.

The Cisco SEA application is successfully uploaded to SD-WAN Manager and appears as an entry in **Virtual Images**, ready for deployment to your network devices.

Create a configuration group profile with an SEA feature

Configure a Configuration Group Profile with a Secure Equipment Access (SEA) feature to enable connectivity between the Cisco SEA agent and the physical interface of the host device.

Create and configure a Configuration Group Profile that includes an SEA feature to establish communication between the Cisco SEA agent and the host device interface, enabling access to the Cisco SEA cloud portal.

The Secure Equipment Access (SEA) feature enables secure remote access to network equipment through the Cisco SEA cloud portal. This configuration establishes the necessary connection between the SEA agent and the physical interface using virtual port group (VPG) 7.

Before you begin

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

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

as the solution type.

Follow these steps to create a Configuration Group Profile with an SEA feature:

Procedure

---

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. Create and configure an SEA feature in an Other profile.
   a. Enter a name and description for the feature.

Table 11: 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.

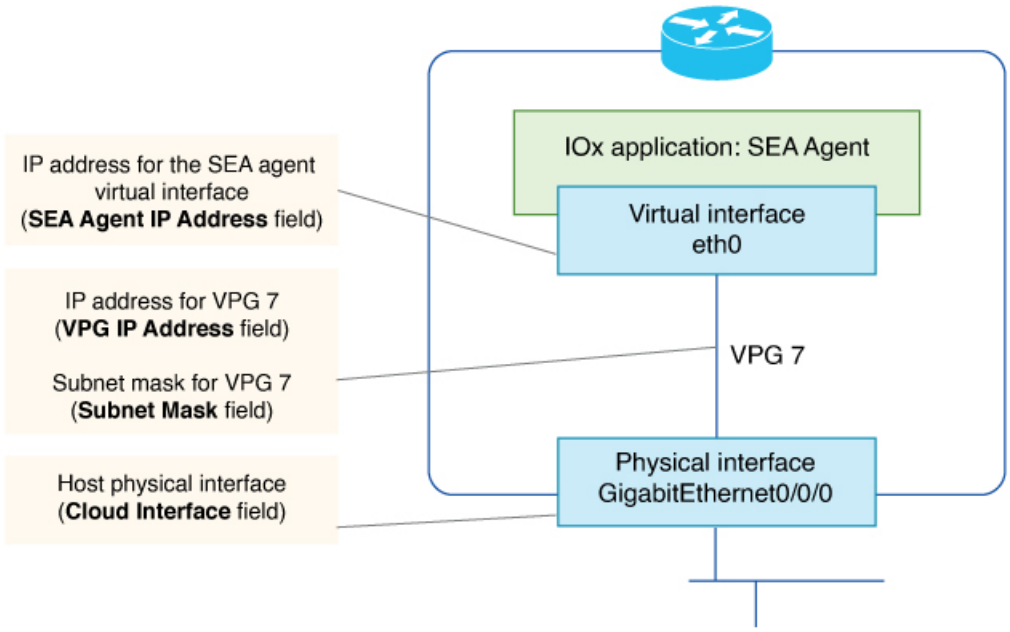


Table 12: Base Configuration

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
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

Field	Description
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 13: 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.
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.

Field	Description
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 14: 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.

You have successfully created a Configuration Group Profile with an SEA feature. The profile enables secure communication between the Cisco SEA agent and the host device interface through virtual port group 7, providing access to the Cisco SEA cloud portal.

What to do next

Also see Deploy a configuration group.

Add a Cisco SEA feature to a configuration group

Configure a Cisco SEA feature by adding it to an existing configuration group through the Cisco SD-WAN Manager interface.

Add a Cisco SEA feature to a configuration group to enable security enforcement and analytics capabilities within your SD-WAN deployment.

Use this procedure when you need to integrate Cisco SEA functionality into your existing SD-WAN or SD-Routing configuration groups. This allows you to apply security policies and analytics features to your network devices.

Before you begin

Follow these steps to add a Cisco SEA feature to a configuration group:

Procedure

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

3. Click the **Configuration Groups** tab.
4. If you need to create a configuration group, follow the steps described in the Using Configuration Groups section of the *Cisco Catalyst SD-WAN Configuration Groups Reference Guide*.
5. For an existing configuration group, click **Add Profile** and add an **Other Profile** to the configuration group.
6. In the configuration group, locate the **Other Profile** drop-down list and choose a Cisco SEA profile.

The Cisco SEA feature is successfully added to the configuration group and can be applied to devices within your network deployment.

Deploy a configuration group with a Cisco SEA feature

Configure a configuration group with the Cisco SEA feature to enable Cisco SEA functionality on devices in your network.

Deploy a configuration group that includes the Cisco SEA feature to enable Cisco SEA functionality on devices in your SD-WAN network. This enables devices to operate as part of the Cisco SEA solution and connect to the Cisco SEA cloud portal.

When deploying a configuration group with the Cisco SEA feature, devices must have network reachability to the Cisco SEA cloud portal before deployment. The deployment process triggers the installation of the Cisco SEA application on devices, which takes several minutes to complete.

Before you begin

- See Supported platforms for Cisco secure equipment access integration on page 26 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 26.

> **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.

Follow these steps to deploy a configuration group with a Cisco SEA feature:

Procedure

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

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.

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.

The configuration group with the Cisco SEA feature is deployed to the selected devices. Devices install the Cisco SEA application and establish a connection to the Cisco SEA cloud portal. After successful deployment, devices operate as part of the Cisco SEA solution.

Verify the Cisco Secure Equipment Access integration

Outlines the process for verifying the integration of Cisco Secure Equipment Access.

Verify the Secure Equipment Access connection

Verify that devices with deployed Cisco SEA features have successfully connected to the Cisco Secure Equipment Access cloud portal.

Confirm that devices have successfully installed the Cisco SEA application and are operating as part of the Cisco SEA solution after deploying configuration groups with Cisco SEA features.

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 35.

Procedure

---

1. Log in to the Cisco SEA cloud portal.
2. View the device list. For details, see the Cisco Secure Equipment Access documentation on the Cisco DevNet site.

The device list displays devices that have successfully connected to the Cisco SEA cloud portal, confirming that the Cisco SEA application installation was successful and the devices are operating as part of the Cisco SEA solution.

Verify the Secure Equipment Access application using the CLI

Verify that the Cisco Secure Equipment Access application is running correctly on SD-WAN or SD-Routing devices by checking IOx services and application status through CLI commands.

This task helps you confirm that the Cisco Secure Equipment Access application has been successfully deployed and is functioning properly on your network devices.

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 35.

Follow these steps to verify that the Cisco Secure Equipment Access application is operating on a device:

Procedure

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

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

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 35.

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
```

You have confirmed whether the Cisco Secure Equipment Access application is operating correctly on the device. If both commands show the services and application in a running state, the verification is successful.

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

Configure monitoring for the Cisco Secure Equipment Access application to view resource usage and operational details on SD-WAN devices.

Monitor the Cisco Secure Equipment Access application to track its performance, resource usage, and operational status on deployed devices.

This monitoring capability enables you to view detailed information about the Cisco Secure Equipment Access application running on devices in your SD-WAN environment. You can check resource utilization, network interfaces, storage usage, and other operational details.

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 35.

Follow these steps to monitor the Cisco Secure Equipment Access application on devices:

Procedure

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

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

You can now view real-time monitoring data for the Cisco Secure Equipment Access application, including resource utilization, network status, and operational details.

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

Topics:

- Feature history for Third-party custom application integration with Cisco Catalyst SD-WAN
- Third-party custom application integration with Cisco Catalyst SD-WAN
- Supported platforms for third-party custom application integration
- Prerequisites for third-party custom application integration
- Restrictions for third-party custom application integration
- Configure third-party custom application integration
- Verify that a third-party custom application using the CLI
- Monitor a third-party custom application on devices

Describes how to integrate third-party custom applications with the platform to extend functionality and create seamless workflows between external systems and native capabilities.

Feature history for Third-party custom application integration with Cisco Catalyst SD-WAN

Provides information about third-party custom application integration with Cisco Catalyst SD-WAN.

This reference provides feature history for third-party custom application integration with Cisco Catalyst SD-WAN.

Table 15: 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.

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

Explains third-party custom application integration with Cisco Catalyst SD-WAN.

Third-party custom application integration is a functionality that allows Cisco SD-WAN Manager to support integration with third-party-developed Cisco IOx applications that

- operate on devices in Docker containers
- add functionality to devices that run Cisco IOS XE Catalyst SD-WAN software, and
- may include connectivity to other data sources and components.

Connectivity options

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 44.

- An application server

  See the network configuration parameters in Create a configuration group profile with a custom application feature on page 44.

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

Lists supported platforms for third-party application integration.

This reference provides information about the platforms that support third-party custom application integration, including specific router models and their supported software versions.

Table 16: 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

Outlines the resource requirements that must be met before integrating third-party custom applications with devices.

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

Outlines 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 49.

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

Multitenancy has restrictions for third-party custom applications.

- 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

Configure third-party custom application integration at a high level to enable monitoring and management of custom applications on devices.

This task enables you to integrate third-party custom applications with your SD-WAN infrastructure to extend device functionality and monitoring capabilities.

Third-party application integration allows you to deploy and manage custom applications on SD-WAN devices through a series of configuration steps that prepare the device environment, upload application images, and create deployment profiles.

Procedure

1. Activate Cisco IOx on devices on page 42
2. Upload the third-party custom application to Cisco SD-WAN Manager on page 43
3. Create a configuration group profile with a custom application feature on page 44
4. Add a custom application feature to a configuration group on page 47
5. Deploy a configuration group with a custom application feature on page 48

The third-party custom application integration is configured and ready for deployment on your SD-WAN devices.

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 50.

Activate Cisco IOx on devices

Configure Cisco IOx activation on devices to enable third-party custom Cisco IOx applications.

This procedure activates Cisco IOx on devices to enable running third-party custom Cisco IOx applications.

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.

Follow these steps to activate Cisco IOx on devices:

Procedure

1. Create a configuration group with a CLI add-on profile.
2. In the CLI add-on profile, include the **iox** command to activate Cisco IOx.

```
iox
```

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

Cisco IOx is activated on the devices and ready to run third-party custom Cisco IOx applications.

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

Configure third-party custom application hosting by uploading the application image to either the SD-WAN Manager local repository or a remote repository server.

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

Third-party custom applications can be hosted in either a local or remote repository depending on your environment configuration and requirements. The local repository option is available in single-tenant environments or for service providers operating multitenant environments, while the remote repository option provides flexibility for tenants when applications are not available locally.

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 17: 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.

Elements	Description
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

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.

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 the information about registering a remote server in the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*.
   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 third-party custom application, making it available for deployment to compatible devices in your network.

Create a configuration group profile with a custom application feature

Configure a configuration group profile with a custom application feature to enable third-party-developed applications in SD-WAN or SD-Routing environments.

Create a configuration group profile that incorporates a custom application feature to support third-party-developed applications in your network environment.

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.

Follow these steps to create a configuration group profile with a custom application feature:

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. Create and configure a Custom Application feature in an Other profile.
   a. Enter a name and description for the feature.

      Table 18: Name and Description

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

   b. The basic settings are mandatory.

      Table 19: 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 20: 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 21: 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 22: 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 23: 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.

You have successfully created a configuration group profile with a custom application feature that is configured to support third-party applications according to their specific requirements.

What to do next

Also see Deploy a configuration group.

Add a custom application feature to a configuration group

Configure a Custom Application profile by adding it to an existing configuration group or creating a new one.

Add Custom Application features to configuration groups to apply custom application policies across multiple devices in your SD-WAN network.

Custom Application profiles allow you to define application-specific policies that can be deployed consistently across devices within a configuration group. This task applies to both SD-WAN and SD-Routing solutions.

Before you begin

Follow these steps to add a Custom Application feature to a configuration group:

Procedure

---

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

3. Click the **Configuration Groups** tab.
4. If you need to create a configuration group, follow the steps described in Using Configuration Groups in the *Cisco Catalyst SD-WAN Configuration Groups Reference Guide*.
5. For an existing configuration group, click **Add Profile** and add an **Other Profile** to the configuration group.
6. In the configuration group, locate the **Other Profile** drop-down list and choose a Custom Application profile.

The Custom Application profile is added to the configuration group and can now be deployed to devices associated with this group.

Deploy a configuration group with a custom application feature

Configure a configuration group deployment with a custom application feature to devices in your SD-WAN network.

Deploy a configuration group that includes a custom application feature to devices in your SD-WAN network to enable custom application functionality.

Configuration groups allow you to deploy standardized configurations with custom applications across multiple devices in your SD-WAN network. This process includes activating Cisco IOx on target devices and monitoring the deployment progress.

Before you begin

See Supported platforms for third-party custom application integration on page 40 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 42.

Follow these steps to deploy a configuration group with a custom application feature:

Procedure

1. Use the configuration group deployment procedure in the *Cisco Catalyst SD-WAN Configuration Groups Reference Guide* to deploy a configuration group to devices in the network.
2. If you are deploying to devices of the SD-WAN solution type, during deployment, enter any required device-specific variables for each router.
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.

The configuration group with the custom application feature is successfully deployed to the selected devices. The custom application is installed and activated on the devices, enabling the configured functionality.

Uninstall a third-party custom application

Configure the removal of a third-party-developed custom application from devices by removing the Custom Application feature from the configuration group and deploying the changes.

Uninstall a third-party-developed custom application that has been previously deployed to devices.

Uninstalling a third-party-developed custom application presumes that you have installed the application already. See Configure third-party custom application integration on page 42.

Procedure

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.
2. Deploy the configuration group to devices. See Deploy a configuration group with a custom application feature on page 48.

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

Verify that a third-party custom application using the CLI

Verify that a third-party custom application is running correctly on a device by using CLI commands to check the IOx service status and application state.

This task verifies that a deployed third-party custom application is functioning correctly on a device in the SD-WAN or SD-Routing solutions.

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 48.

Follow these steps to verify that a third-party custom application is operating on a device using the CLI:

Procedure

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

   Example

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

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 48.

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.

Example

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

The command output displays the application state. If the state shows as RUNNING for the specified application ID, the third-party custom application is operating correctly on the device.

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 44. 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

Configure monitoring of third-party custom applications on devices using App Hosting commands to view resource usage and application details.

Monitor the resource usage and operational details of third-party custom applications deployed on devices in the SD-WAN solution.

This monitoring capability applies to devices in the SD-WAN solution but not to devices in the SD-Routing solution. You can use various App Hosting commands to view different aspects of application performance and resource consumption.

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 48.

Procedure

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

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

The system displays the requested information about the custom applications running on the device, including resource usage, network utilization, storage utilization, and other operational details based on the selected App Hosting command.

4 Cisco Unified Communications Voice Services

Topics:

- Feature history for Cisco unified communications voice services
- Cisco unified communications voice services
- Configure unified communications voice services
- Provision a device template for unified communications
- Dial peer CSV file
- Translation rules CSV file
- Monitor UC operations

Describes the voice communication capabilities and services provided by Cisco Unified Communications platform for enterprise telephony, including call routing, voice messaging, and integration with collaboration tools.

Feature history for Cisco unified communications voice services

Provides the release history and descriptions of features for Cisco Unified Communications Voice Services on supported routers.

This reference provides the chronological development and feature additions for Cisco Unified Communications Voice Services, including release information and feature descriptions for each implementation milestone.

Table 24: Feature history

Feature Name	Release Information	Description
Cisco IP-based media services	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	You can now enable Cisco IP-based media services using a feature template.
Cisco Unified Communications Voice Services	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	This feature enables you to configure Cisco Unified Communications (UC) voice services on supported routers using feature templates and voice policies. When enabled, these routers can process calls for various endpoints, including voice ports, POTS dial peers, SIP dial peers, and phone profiles in Cisco Unified SRST mode. You configure UC voice services from the Feature tab and the Voice Policy page for a supported device. To configure UC voice services, Cisco SD-WAN Manager must run Cisco vManage 20.1.1. This feature is supported on Cisco 4000 Series Integrated Services Routers.
DSP Farms for UC Voice Services with Workflow Library and Configuration Groups	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	You can now configure DSP farms for UC voice services using the Workflow Library and configuration groups.

Cisco unified communications voice services

Describes Cisco Unified Communications voice services that enable configuration of feature templates and voice policies for supported routers.

Cisco Unified Communications voice services are router capabilities that

- enable configuration of feature templates and voice policies for Foreign Exchange Office (FXO), Foreign Exchange Station (FXS), FXS/Direct Inward Dialing (DID) interfaces, and Primary Rate Interface (PRI) Integrated Services Digital Network (ISDN)
- support DSPFarm feature template to enable Cisco IP-based media services, and

- allow routers to process calls for various endpoints including voice ports for analog and digital interfaces, Plain Old Telephone Service (POTS) dial peers, Session Initiation Protocol (SIP) dial peers, and phone profiles in Cisco Unified Survivable Remote Site Telephony (SRST) mode.

System requirements

To configure UC voice services for Cisco Unified Communications, Cisco SD-WAN Manager must run Cisco SD-WAN Release 20.3.1 or later.

Starting with Cisco IOS XE Catalyst SD-WAN Release 17.3.1a, you can also configure parameters for Primary Rate Interface (PRI) Integrated Services Digital Network (ISDN).

Note

Starting with Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, you can also configure and enable UC voice services using the Workflow library or configuration groups. For more information, see Cisco Unified Communications Voice Profile.

For detailed information about commands to configure and maintain Cisco IOS voice applications, see the Cisco IOS Master Command List.

Configure unified communications voice services

Configure Unified Communications Voice Services to enable supported routers to process calls for various endpoints including voice ports, POTS dial peers, SIP dial peers, and phone profiles.

This task provides the comprehensive workflow to enable Cisco Unified Communications (UC) voice services for supported routers, allowing them to process calls for various endpoints including voice ports, POTS dial peers, SIP dial peers, and phone profiles in Cisco Unified SRST mode.

This ensures that Cisco IOS XE Catalyst SD-WAN devices can process calls for various endpoints and integrate IP-based media services.

Before you begin

Ensure that Cisco Catalyst SD-WAN Manager runs Cisco vManage Release 20.3.1 or later.

Follow these steps to configure Unified Communications Voice Services:

Procedure

1. Add a voice card feature template.

   Configures analog and PRI ISDN digital interfaces for voice cards. See Add a voice card feature template on page 56

2. Add a call routing feature template.

   Configures parameters for TDM-SIP trunking and dial plans. See Add call routing feature template on page 65

3. Add an SRST feature template.

   Configures parameters for Cisco Unified Survivable Remote Site Telephony (SRST) for SIP. See Add an SRST feature template on page 69.

4. Add a DSPFarm Feature Template.

Sets up and provisions a Digital Signal Processor (DSP) farm for media services like transcoding and conferencing. See Add a DSPFarm feature template on page 71

5. Add a voice policy.

   Defines how the system augments and manipulates calls for various endpoint types. See Add a voice policy on page 81.

6. Provision a device template for Unified Communications.

   Selects UC-specific feature templates and sets up the voice policy to include with the device template. See Provision a device template for unified communications on page 118.

After completing this supertask, UC voice services will be enabled on supported Cisco IOS XE Catalyst SD-WAN devices, allowing them to process calls for various endpoints.

What to do next

To monitor the real-time statuses of lines, calls, interfaces, and related items that a device processes, navigate to **Monitor** > **Devices** from the SD-WAN Manager menu.

Add a voice card feature template

Configure a voice card feature template to set up analog and PRI ISDN digital interfaces for voice services on supported routers.

A voice card feature template configures analog and PRI ISDN digital interfaces, which provide configuration settings for ports on voice cards in routers.

When you add a voice card feature template, you configure the type of voice card, port information, and service provider parameters for analog interfaces. For digital interfaces, you configure the type of voice card, the T1 or E1 controller, and related parameters. SD-WAN Manager assists with module placement by displaying available slots and sub-slots based on the device model.

Before you begin

Ensure you have selected the supported device to which you want to add voice services in Cisco SD-WAN Manager.

Follow these steps to add a voice card feature template:

Procedure

---

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**, and click **Add Template**.

   In Cisco vManage Release 20.7.1 and earlier releases, **Feature Templates** is called **Feature**.

3. Select the supported device to which you want to add voice services.
4. Select **Voice Card** from the **Unified Communications** templates.
5. In **Template Name**, enter a name for the template.

   This field may contain uppercase and lowercase letters, digits 0 through 9, hyphens (-), and underscores (_).

6. In **Description**, enter a description for the template.

   This field can contain any characters and spaces.

7. To configure an analog interface, click **New Analog Interface** and configure interface options as described in the Voice card analog interface configuration options on page 58 topic.

From Cisco IOS XE Catalyst SD-WAN Release 17.3.1a, select **Analog Interface** in the Interface area to access **New Analog Interface**.

You can add as many analog interfaces as needed, based on the number of interfaces that your module supports. After you configure each analog interface, click **Add**.

If any analog interfaces are already configured, they appear in the interfaces table on this page. To edit an existing interface, click **...** and select its pencil icon to edit the options in the window that pops up as described in the Voice card analog interface configuration options on page 58 topic, and click **Save Changes**. To delete an interface, click **...** and click the trash can icon.

8. To configure a PRI ISDN digital interface, in the **Interface** area, click **Digital Interface**, click **New Digital Interface**, and configure interface options as described in the Voice card digital interface configuration options on page 59 topic.

   Based on the number of interfaces that your module supports, you can add as many PRI ISDN digital interfaces as needed. After you configure each PRI ISDN digital interface, click **Add**.

   If any digital interfaces are already configured, they appear in the interfaces table on this page. To edit an existing interface, click **...** and select its pencil icon to edit the options in the window that pops up as described in the Voice card digital interface configuration options on page 59 topic, and click **Save Changes**. To delete an interface, click **...**, and click its trash can icon.

   > **Note**
   >
   > After you save the interface configuration, you cannot change the module type, interface type, slot or sub-slot, or time slots.
   >
   > If you want to change time slots, you must delete the interface and create a new one.
   >
   > If you want to change the module type, interface type, and slot or sub-slot, detach the template from the device, unmap the voice policies that are associated with the interfaces, and delete all interfaces that are associated with the module and slot or sub-slot. Next, push the template to the device, reload the device, and create new required interfaces. Finally, push the new template to the device, and reattach the template to the device.

9. Click **Save**.
10. (Optional) To configure additional analog or PRI ISDN digital interfaces for this template:

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

    Click **Feature Templates**.

    In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is called **Feature**.

    Click **...** for the template you wish to configure, and click **Edit**.

    Repeat Step 7 or Step 8 and Step 9.

A voice card feature template is successfully added and configured.

What to do next

If you need to configure more analog or PRI ISDN digital interfaces for this template later, you can edit the template by navigating to **Configuration** > **Templates** > **Feature Templates**, clicking **...** next to the template name, and selecting **Edit**. You can then repeat the configuration steps for analog or digital interfaces.

Voice card analog interface configuration options

Lists the various options available for configuring analog interfaces ON voice cards within Cisco Unified Communications Voice Services.

This reference topic describes the various options available for configuring analog interfaces ON voice cards within Cisco Unified Communications Voice Services. These options allow you to define the type of voice module, port characteristics, and service provider parameters for analog voice ports.

Analog interface configuration options

This table describes the options for configuring an analog interface.

Table 25: Analog interface options

Option	Description	Cisco IOS CLI Equivalent
Module	Select the type of voice module that is installed in the router.	–
Module Slot/Sub-slot	Enter the slot and sub-slot of the voice module.	**voice-card** *slot/subslot*
Use DSP	Enable this option if you want to use the built-in DSPs ON the network interface module for TDM calls.	**no local-bypass**
Port Type	Select the type of ports ON the voice module that you are configuring for this interface (**FXS** or **FXO**). You can select **All** to define the port type for all ports of the selected type, or **Port Range** to define the port type for a specified range of ports. Using Port Range, you can create analog interfaces as described later in this procedure to configure different ranges of ports.	–
Description	Enter a description of the selected port or ports. For example, fax machine or paging system.	**description** *string*
Secondary Dialtone	Available if you select FXO from the Port Type drop-down list. Set to **ON** if you want the selected ports to generate a secondary dial tone when callers access an outside line.	**secondary dialtone**
Connection PLAR	Enter the Private Line Automatic Ringdown extension to which the selected ports forward inbound calls.	**connection PLAR** *digits*
OPX	Available if you select FXO from the Port Type drop-down list. Check this option if you want to enable Off-Premises Extension for the PLAR extension.	**connection PLAR OPX** *digits*

Option	Description	Cisco IOS CLI Equivalent
Signal Type	Select the Signal Type that indicates an ON-hook or off-hook condition for calls that the ports receive. Options are **Loopstart**, **Groundstart**, or **DID**. The DID option is available if you select FXS from the Port Type drop-down list.	**signal** {groundstart | loopstart} **signal DID** {delay-dial | immediate | wink-start}
Caller-ID Enable	Available if you select a signal type of Loopstart or Groundstart. Set to **ON** if you want to enable caller ID information for inbound calls.	**caller-ID enable**
DID Signal Mode	Available if you select a signal type of DID. Choose the mode for the DID signal type (**Delay Dial**, **Immediate**, or **Wink Start**). Default: Wink Start.	**signal DID** {delay-dial | immediate | wink-start}
Shutdown	Set to **ON** if you want to shut down ports that are not being used. Default: Off.	**shutdown**

Voice card digital interface configuration options

Voice Card Digital Interface

This reference topic describes the various options available for configuring digital interfaces on voice cards within Cisco Unified Communications Voice Services. These options allow you to define the type of T1/E1 voice module, interface characteristics, clock sources, and other parameters for digital voice ports.

Digital Interface Configuration Options

This table describes the options for configuring a digital interface.

Table 26: Digital Interface Options

Option	Description	Cisco IOS CLI Equivalent
Digital Interface Tab		
Provides options for configuring parameters for a T1/E1 voice module and the clock source for the module ports. Before you configure these options, ensure that you have the appropriate DSP module installed for each T1/E1 voice module.		
Module	Select the type of T1/E1 voice module that is installed in the router.	–
Interface Type	Select the type of interface on the voice module: • **T1 PRI** –Specifies T1 connectivity of 1.544 Mbps through the telephone switching network, using AMI or B8ZS coding • **E1 PRI** –Specifies a wide-area digital transmission scheme used predominantly in Europe that carries data at a rate of 2.048 Mbps	**card type** { **t1** | **e1** } *slot sub-slot*

Option	Description	Cisco IOS CLI Equivalent
Slot/Sub-slot	Enter the slot and sub-slot of the voice module.	**voice-card** *slot* / *sub-slot*
Use DSP	Enable this option if you want to use the built-in DSPs on the network interface module for TDM calls.	**no local-bypass**
Interface	Perform these actions to configure the number of T1/E1 ports to be provisioned on the module, and the clock source for each port: 1. Click **Add** . The Port and Clock Selector window displays. 2. Check the check box that corresponds to each port that you want to configure. The number of ports that you can configure depends on the Module type that you select. 3. For each port, select the clock source: • **Line** –Sets the line clock as the primary clock source. With this option, the port clocks its transmitted data from a clock that is recovered from the line receive data stream. • **Primary Clock** –Sets the port to be a primary clock source. • **Secondary Clock** –Sets the port to be a secondary clock source. • **Network** –Sets the backplane clock or the system oscillator clock as the module clock source. We recommend that you set one port to be the primary clock and set another port going to the same network as a secondary clock source to act as a backup. 4. Click **Add** .	**controller** { **t1** | **e1** } *slot* / *sub-slot* / *number* **clock source** { **network** | **line** | **line primary** | **line secondary** }
Network Participation	This check box displays after you add an interface. Check this check box to configure the T1/E1 module to participate in the backplane clock. Uncheck this check box to remove the clock synchronization with the backplane clock for the module. By defult, this check box is checked.	**network-clock synchronization participate** *slot* / *sub-slot*

Option	Description	Cisco IOS CLI Equivalent
Shutdown	Perform these actions to disable or enable the controller, serial interface, or voice port that is associated with the interface port. 1. Click **Shutdown Selected** . The Shutdown window displays. 2. For each port, select the item or items that you want to enable (**Controller** , **Serial** , or **Voice Port** . If you do not select an item, it is enabled. 3. Click **Add** .	**controller e1/t1** *slot* / *sub-slot* / *port* **shutdown** **interface serial** *slot* / *sub-slot* / **port:** { **15** | **23** } **shutdown** **voice-port** *slot* / *sub-slot* / **port:** { **15** | **23** } **shutdown**
Time Slots	Select the number of time slots of the interface type. Valid ranges: • For T1 PRI–Time slots 1 through 24. The 24th time slot is the D channel. • For E1 PRI– Time slots 1 through 31. The 16th time slot is the D channel.	**controller e1/t1** *slot* / *sub-slot* / *port* **pri-group timeslots** *timeslot-range* [**voice-dsp**]
Framing	Select the frame type for the interface type. For a T1 PRI interface type, options are: • **esf** –Extended super frame (default) • **sf** –Super frame For an E1 PRI interface type, options are: • **crc4** –CRC4 framing type (default) • **no-crc4** –No CRC4 framing type	**controller t1** *slot* / *sub-slot* / *port* **framing** [**esf** | **sf**] **controller e1** *slot* / *sub-slot* / *port* **framing** [**crc4** | **no-crc4**] [**australia**]
Australia	This check box displays when you select E1 PRI for the interface type. Check this check box to use the **australia** framing type.	**controller e1** *slot* / *sub-slot* / *port* **framing** [**crc4** | **no-crc4**] **australia**

Option	Description	Cisco IOS CLI Equivalent
Line Code	Select the line code type for the interface type. For a T1 PRI interface type, options are: • **ami** –Use Alternate Mark Inversion as the line code type • **b8zs** –Use binary 8-zero substitution as the line code type (default) For an E1 PRI interface type, options are: • **ami** –Use Alternate Mark Inversion as the line code type • **hdb3** –Use high-density binary 3 as the line code type (default)	**controller t1** *slot* / *sub-slot* / *port* **linecode** [**ami** | **b8zs**] **controller e1** *slot* / *sub-slot* / *port* **linecode** [**ami** | **hdb3**]
Line Termination	This check box appears only for an Interface type of E1 PRI. Select the line termination type for the E1 controller: • **75-ohm** –75 ohm unbalanced termination • **120-ohm** –120 ohm balanced termination (default)	**controller e1** *slot* / *sub-slot* / *port* **line-termination** { **75-ohm** | **120-ohm** }
Cable Length Type	This check box appears only for an Interface type of T1 PRI. Select the cable length type for the T1 PRI interface type: • **long** –Long cable length • **short** –Short cable length	**controller t1** *slot* / *sub-slot* / *port* **cablelength** { **short** | **long** }
Cable Length	This check box appears only for an interface type of T1 PRI. Select the cable length for the T1 PRI interface type. Use this option to fine-tune the pulse of a signal at the receiver for a T1 cable. The default value is **0db** .	**controller t1** *slot* / *sub-slot* / *port* **cablelength** { **[short** [**110ft** | **220ft** | **330ft** | **440ft** | **550ft** | **660ft**]] [**long** [**-15db** | **-22.5db** | **-7.5db** | **0db**]]}
Network Side	Enable this option to have the device use the standard PRI network-side interface. By default, this option is disabled (set to **No**).	**interface serial** *slot* / *sub-slot* / **port:** { **15** | **23** } **isdn protocol-emulate** [**network** | **user**]

Option	Description	Cisco IOS CLI Equivalent
Switch Type	Select the ISDN switch type for this interface: • **primary-qsig** –Supports QSIG signaling according tot the Q.931 protocol. Network side functionality is assigned with the isdn protocol-emulate command. • **primary-net5** –NET5 ISDN PRI switch types for Asia, Australia, and New Zealand. ETSI-compliant switches for Euro-ISDN E-DSS1 signaling system. • **primary-ntt** –Japanese NTT ISDN PRI switches. • **primary-4ess** –Lucent (AT&T) 4ESS switch type for the United States. • **primary-5ess** –Lucent (AT&T) 5ESS switch type for the United States. • **primary-dms100** –Nortel DMS-100 switch type for the United States. • **primary-ni** –National ISDN switch type.	**interface serial** *slot* / *sub-slot* / **port:** { **15** | **23** } **isdn switch-type** [**primary-4ess** | **primary-5ess** | **primary-dms100** | **primary-net5** | **primary-ni** | **primary-ntt** | **primary-qsig**]

Option	Description	Cisco IOS CLI Equivalent
ISDN Timer	Perform these actions to configure the ISDN timers for the interface: 1. Click **Add** . The ISDN Timer window displays. 2. Configure the following timers as needed. The values are in milliseconds. • **T200** . Valid range: integers 400 through 400000. Default: 1000. • **T203** . Valid range: integers 400 through 400000. The default value is based on the switch type and network side configurations. • **T301** . Valid range: integers 180000 through 86400000. The default value is based on the switch type and network side configurations. • **T303** . Valid range: integers 400 through 86400000. The default value is based on the switch type and network side configurations. • **T306** . Valid range: integers 400 through 86400000. Default: 30000. • **T309** . Valid range: integers 0 through 86400000. The default value is based on the switch type and network side configurations. • **T310** . Valid range: integers 400 through 400000. The default value is based on the switch type and network side configurations. • **T321** . Valid range: Integers 0 through 86400000. The default value is based on the switch type and network side configurations. 3. Click **Add** .	**interface serial** *slot* / *sub-slot* / **port:** { **15** | **23** } **isdn timer T200** *value* **isdn timer T203** *value* **isdn timer T301** *value* **isdn timer T303** *value* **isdn timer T306** *value* **isdn timer T309** *value* **isdn timer T310** *value* **isdn timer T321** *value*
Delay Connect Timer	Select the duration, in milliseconds, to delay connect a PRI ISDN hairpin call. Valid range: integers 0 through 200. Default: 20.	**voice-port** *slot* / *sub-slot* / **port:** { **15** | **23** } **timing delay-connect** *value*

Clock Tab

Use this tab to configure priority order for the primary and secondary clock sources that you selected for each module.

This tab is vailable after you configure a PRI ISDN digital interface and click **Add** .

Option	Description	Cisco IOS CLI Equivalent
Clock Priority Sorting	Configure the priority of up to six clock sources. The drop-down list displays the interface ports for which a primary or secondary clock source is defined and that is configured for network participation. Check a check box to select the port for inclusion in the priority list, and use the **Up arrow** next to a port to change its priority. The list displays the ports in order of priority, with the port with the highest priority at the top of the list. After you configure the priority, this field displays the selected ports in priority order. We recommend that all ports in the priority list be of the same type, either E1-PRI or T1-PRI.	**network-clock input-source** priority **controller** [**t1** | **e1**] *slot* / *sub-slot* / *port*
Automatically Sync	Select **Add** to enable network synchronization between all modules and the router. Default: **On** .	network-clock synchronization automatic
Wait to restore clock	Enter the amount of time, in milliseconds, that the router waits before including a primary clock source in the clock selection process. Valid range: 0 through 86400. Default: 300.	network-clock wait-to-restore *milliseconds*

Add call routing feature template

Configure a call routing feature template that defines parameters for TDM-SIP trunking, trusted IP addresses for preventing toll fraud, and dial plans.

A call routing feature template configures parameters for TDM-SIP trunking, including trusted IP addresses for preventing toll fraud, and a dial plan.

A dial plan, made up of dial peers, defines how a router routes traffic to and from voice ports to the PSTN or to another branch. This template allows for the definition of global SIP communication settings and detailed dial peer configurations.

Before you begin

Ensure you have selected the supported device to which you want to add call routing features in Cisco SD-WAN Manager.

Follow these steps to add a call routing feature template:

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**, and click **Add Template**.

   In Cisco vManage Release 20.7.1 and earlier releases, **Feature Templates** is called **Feature**.
3. Select the supported device to which you want to add voice services.
4. Select **Voice Card** from the **Unified Communications** templates.
5. In **Template Name**, enter a name for the template.

This field may contain uppercase and lowercase letters, digits 0 through 9, hyphens (-), and underscores (_).

6. In **Description**, enter a description for the template.

   This field can contain any characters and spaces.

7. In **Global**, configure options as described in the Global call routing options on page 66 topic.
8. In **Dial Plan**, perform one of these actions:

   To configure a dial peer directly, configure options as described in the Dial peer options on page 67 topic.

   To create or edit a dial peer CSV file, click **Download Dial Peer List** to download the system provided file named Dial-Peers.CSV. The first time you download this file, it contains field names but no records. Update this file as needed by using an application such as Microsoft Excel. For more information about this file, see Dial peer CSV file on page 121.

   To import configuration information from a dial peer CSV file that you have created, click **Upload Dial Peer List**.

   You can add as many dial peers as needed. Click **Add** after you configure each dial peer. If any dial peers already are configured, they appear in the dial peers table on this page. To edit a configured dial peer, click **...**, and click its pencil icon. Edit the options in the window that pops up as described in the table, and click **Save Changes**. To delete a dial peer, click **...**, and click its trash can icon.

9. Click **Save**.

A call routing feature template is successfully added and configured.

What to do next

Proceed to add an SRST feature template if required for your Unified Communications deployment.

Global call routing options

Lists the global options available for configuring call routing parameters within a call routing feature template.

This reference topic describes the global options available for configuring call routing parameters within a call routing feature template. These settings define how the router communicates through SIP and handles trusted IP addresses for call security.

Global call routing options

This table describes global options for configuring call routing.

Table 27: Global call routing options

Option	Description	Cisco IOS CLI Equivalent
Trusted IPv4 Prefix List	Enter the IPv4 addresses with which the router can communicate through SIP. Enter each IPv4 address in CIDR format. For example, 10.1.2.3/32. Separate each address with a comma (,). The router does not communicate with other IPv4 addresses, which prevents fraudulent calls being placed through the router. A Trusted IPv4 Prefix is required for TDM to IP calls.	**voice service voip** **IP address trusted list** **ipv4** *ipv4-address|ipv4-network-mask*

Option	Description	Cisco IOS CLI Equivalent
Trusted IPv6 Prefix List	Enter the IPv6 addresses with which the router can communicate through SIP. Separate each IPv6 address with a comma (,). The router does not communicate with other IPv6 addresses, which prevents fraudulent calls being placed through the router. A Trusted IPv6 Prefix is required for TDM to IP calls.	**voice service voip** **IP address trusted list** **ipv6** *ipv6-prefix*/*prefix-length*
Source Interface	Enter the name of the source interface from which the router initiates SIP control and media traffic. This information defines how the return/response to this traffic should be sent.	**voice service voip** **SIP** **bind control source-interface** *interface-id* **bind media source-interface** *interface-id*

Dial peer options

Lists the various options available for configuring dial peers, which are essential components of a dial plan.

This reference topic describes the various options available for configuring dial peers, which are essential components of a dial plan. Dial peers define how a router routes traffic for voice calls, including settings for incoming/outgoing calls and transport protocols.

Dial peer options

This table describes options for configuring dial peers.

Table 28: Dial peer options

Option	Description	Cisco IOS CLI Equivalent
Voice Dial Peer Tag	Enter a number to be used to reference the dial peer.	**dial-peer voice** *number* {**POTS** | **voip**}
Dial Peer Type	Select the type of dial peer that you are creating (**POTS** or **SIP**).	**dial-peer voice** *number* {**POTS** | **voip**}
Direction	Select the direction for traffic on this dial peer (**Incoming** or **Outgoing**).	Incoming: dial-peer voice *number* {POTS | voip} **incoming called-number** *string* Outgoing: dial-peer voice *number* {POTS | voip} **destination-pattern** *string*
Description	Enter a description of this dial peer.	**description**

Option	Description	Cisco IOS CLI Equivalent
Numbering Pattern	Enter a string that the router uses to match incoming calls to the dial peer. Enter the string as an E.164 format regular expression in the form [0-9,A-F#*.?+%()-]*T?.	Incoming: dial-peer voice *number* {POTS | voip} **incoming called-number** *string* Outgoing: dial-peer voice *number* {POTS | voip} **destination-pattern** *string*
Forward Digits Type	Available if you select the POTS dial peer type and the Outgoing direction. Select how the dial peer transmits digits in outgoing numbers: • **All**–The dial peer transmits all digits • **None**–The dial peer does not transmit digits that do not match the destination pattern • **Some**–The dial peer transmits the specified number of right-most digits Default: None.	All: dial-peer voice *number* POTS **forward-digits all** None: dial-peer voice *number* POTS **forward-digits 0** Some: dial-peer voice *number* POTS **forward-digits** *number*
Forward Digits	Available if you select **Some** for Forward Digits Type. Enter the number of right-most digits in the outgoing number to transmit. For example, if you set this value to 7 and the outgoing number is 1112223333, the dial peer transmits 2223333.	dial-peer voice *number* POTS **forward-digits** *number*
Prefix	Available if you select the POTS dial peer type and the Outgoing direction. Enter digits to be prepended to the dial string for outgoing calls.	dial-peer voice *number* POTS **prefix** *string*
Transport Protocol	Available if you select SIP for the Dial Peer Type. Choose the transport protocol (**TCP** or **UDP**) for SIP control signaling.	dial-peer voice *number* voip **session transport** {**TCP** | **UDP**}
Preference	Available if you select POTS or SIP for the Dial Peer Type. Select an integer from 0 to 10, where the lower the number, the higher the preference. If dial peers have the same match criteria, the system uses the one with the highest preference value. Default: 0 (highest preference).	dial-peer voice *number* voip **preference** *value* dial-peer voice *number* POTS **preference** *value*

Option	Description	Cisco IOS CLI Equivalent
Voice Port	Available if you select the POTS dial peer type. Enter the voice port that the router uses to match calls to the dial peer. For an analog port, enter the port you want. For a digital **T1** PRI ISDN port, enter a port with the suffix:**23**. For a digital E1 PRI ISDN port, enter a port with the suffix :**15**. For an outgoing dial peer, the router sends calls that match the dial peer to this port. For an incoming dial peer, this port serves as an extra match criterion. The dial peers are matched only if a call comes in on this port.	dial-peer voice *number* POTS For an analog port: **port** *slot*/*subslot*/*port* For a digital port: **port** *slot*/*subslot*/*port*:**15** **port** *slot*/*subslot*/*port*:**23**
Destination Address	Available if you select the SIP dial peer type and the Outgoing direction. Enter the network address of the remote voice gateway to which calls are sent after a local outgoing SIP dial peer is matched. Enter the address in one of these formats: • dns:*hostname.domain* • *SIP-server* ipv4:*destination-addres* ipv6:*destination-address*	**session target** {**ipv4:***destination-address* | **ipv6:***destination-address*| **SIP-server** | **dns:***hostname.domain*}

Add an SRST feature template

Add an SRST feature template

An SRST feature template configures parameters for Cisco Unified Survivable Remote Site Telephony (SRST) for SIP. With Cisco Unified SRST, if the WAN goes down or is degraded, SIP IP phones in a branch site can register to the local gateway so that they continue to function for emergency services. Use this procedure to add and configure such a template.

The SRST feature template allows you to define global SRST settings, such as system messages and maximum phone/directory numbers, as well as individual phone profiles for SIP phones.

•

Before you begin

Ensure you have selected the supported device to which you want to add Cisco Unified SRST features in Cisco SD-WAN Manager.

Follow these steps to add an SRST feature template:

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**, and click **Add Template**.

   In Cisco vManage Release 20.7.1 and earlier releases, **Feature Templates** is called **Feature**.

3. Select the supported device to which you want to add Cisco Unified SRST features.
4. Click **SRST** from the Unified Communications templates.
5. In **Template Name**, enter a name for the template.

   This field can contain uppercase and lowercase letters, digits 0 through 9, hyphens (-), and underscores (_).
6. In **Description**, enter a description for the template.

   This field can contain any characters and spaces.
7. In **Global Settings**, configure options as described in the Global Cisco Unified SRST Options on page 70 topic.
8. From **Phone Profile**, click **New Phone Profile** to create a phone profile, and configure options as described in the SRST Phone profile options on page 71 topic.

   A phone profile provides pool tag and device network information for a SIP phone.

   You can add as many phone profiles as needed. Click **Add** after you configure each phone profile.

   If any phone profiles already are configured, they appear in the phone profiles table on this page. To edit a configured phone profile, click **...**, and click its pencil icon. Edit the options in the window that pops up as described in the table, and click **Save Changes**. To delete a phone profile, click **...**, and click its trash can icon.
9. Click **Save**.

An SRST feature template is successfully added and configured.

What to do next

Proceed to add a DSPFarm Feature Template if required for your Unified Communications deployment.

Global Cisco Unified SRST Options

Details the global configuration options for Cisco Unified SRST, including system messages, phone and directory number capacities, and music on hold settings, along with corresponding Cisco IOS CLI equivalents.

This reference topic describes the global options available for configuring Cisco Unified Survivable Remote Site Telephony (SRST) parameters. These settings define system-wide behaviors for SRST mode, including messages, phone capacity, and music on hold.

Table 29: Global Cisco Unified SRST Options

Option	Description	Cisco IOS CLI Equivalent
System Message	Enter a message that displays on endpoints when Cisco Unified SRST mode is in effect.	**voice register global** **system message** *string*
Max Phones	Enter the number of phones that the system can register to the local gateway when in Cisco Unified SRST mode. The available values and the maximum values that you can enter in this field depend on the device that you are configuring. Hover your mouse pointer over the Information icon next to this field to see maximum values for supported devices.	**voice register global** **max-pool** *max-voice-register-pools*

Option	Description	Cisco IOS CLI Equivalent
Max Directory Numbers	Enter the number of DNs that the gateway supports when in Cisco Unified SRST mode. The available values and the maximum values that you can enter in this field depend on the device that you are configuring. Hover your mouse pointer over the Information icon next to the Max phones to support field to see maximum values for supported devices.	**voice register global** **max-dn** *max-directory-numbers*
Music on Hold	Select **Yes** to play music on hold on endpoints when a caller is on hold when in Cisco Unified SRST mode. Otherwise, select **No**.	–
Music on Hold file	Enter the path and file name of the audio file for music on hold. The file must be in the system flash and must be in .au or .wav format. In addition, the file format must contain 8-bit 8-kHz data, for example, CCITT a-law or u-law data format.	**call-manager-fallback** **moh** *filename*

SRST Phone profile options

Details the configurable options for SRST phone profiles, including settings for voice register pool tags and device network IPv4 and IPv6 prefixes, with corresponding Cisco IOS CLI equivalents for SIP phone registration in SRST mode.

This reference topic describes the options available for configuring individual SRST phone profiles. These settings define the network identification for SIP phones registering to a local gateway in SRST mode.

Table 30: SRST Phone Profile Options

Option	Description	Cisco IOS CLI Equivalent
Voice Register Pool Tag	Enter the unique sequence number of the IP phone to be configured. The maximum value is defined by the Max phones to support option in the Global tab of the SRST feature template.	**voice register pool** *pool-tag*
Device Network IPv6 Prefix	Enter the IPv6 prefix of the network that contains the IP phone to support. For example, a.b.c.d/24.	**voice register pool** *pool-tag* **id** [**network** *address* **mask** *mask*]
Device Network IPv4 Prefix	Enter the IPv4 prefix of the network that contains the IP phone to support.	**voice register pool** *pool-tag* **id** [**network** *address* **mask** *mask*]

Add a DSPFarm feature template

Add a DSPFarm feature template

A DSP farm is a pool of Digital Signal Processor (DSP) resources on a router used by Cisco Unified Communications Manager for controlled transcoding, conferencing (non-secure only), and media termination point (MTP) services. A

DSPFarm feature template is used to set up and provision a DSP farm. Use this procedure to add and configure such a template.

When you add a DSPFarm feature template, you configure options for the following items:

- Media resource modules–DSP modules and their placement on a router. You determine and build DSP farm profiles based on media resource modules.
- DSP farm profiles–Each profile defines parameters for provisioning a specific DSP farm service type. A profile includes options for provisioning a group of DSP resources that is used for transcoding, conferencing (only non-secure conferencing is supported), or MTP services. A profile is registered to a Cisco Unified Communications Manager so that the Cisco Unified Communications Manager can invoke the resources for a service as needed.
- SCCP config–Configures a local interface that is used to communicate with up to four Cisco Unified Communications Manager servers, and configures related information that is required to register the DSP farm profiles to Cisco Unified Communications Manager. Also configures one or more Cisco Unified Communications Manager groups, each of which includes up to four Cisco Unified Communications Manager servers that control the DSP farm services that, in turn, are associated with the servers.

Before you begin

Ensure you have selected the supported device to which you want to add a DSP farm in Cisco SD-WAN Manager.

Follow these steps to add a DSPFarm feature template:

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**, and click **Add Template**.

   > **Note**
   >
   > In Cisco vManage Release 20.7.1 and earlier releases, **Feature Templates** is called **Feature**.

3. Select the supported device to which you want to add a DSP farm.
4. Click **DSPFarm** from the **Unified Communications** templates.
5. In **Template Name**, enter a name for the template.

   This field can contain uppercase and lowercase letters, digits 0 through 9, hyphens (-), and underscores (_).

6. In **Description**, enter a description for the template.

   This field can contain any characters and spaces.

7. Configure the DSPFarm parameters.
   a) From **Media Resources Modules**, click **Add Media Resources**, and configure options as described in the Media resource options on page 73 topic.

   A media resource module is a DSP module that is used by DSP Farm profiles.

   You can add as many media resources interfaces as needed.

   Click **Add** after you configure each media resource. After you configure a media resource, you cannot modify or delete it because other configuration items are based on the module and its placement. If you need to change a media resource configuration, you must remove the DSPFarm feature template and create a new one.

If any media resources are already configured, they appear in the table in this tab. To edit a configured media resource, click **...**, and click its pencil icon. Edit the options in the window that pops up as described in the Media Resource Options table, and click **Save Changes**. To delete a media resource, click **...**, and click its trash can icon.

b) From **Profile**, click **Add New Profile** to add a profile for a DSP farm service on a router, and configure options for the profile as described in the DSPFarm service options on page 73 topic.

Click **Add** after you configure a profile. You can add up to 10 DSP farm profiles for each feature template.

Before you create a profile, you must know the maximum number of sessions that can be configured with the DSP resources that are available on the router. These resources are based on the type of modules in the router. To determine these resources, you can use a DSP calculator.

After you add a profile, you can modify the List Codec, Maximum Sessions, Maximum Conference Participants, and Shutdown options. You cannot change the profile type. If you want to change the profile type, you must delete the profile and create a new one.

If any profiles are already configured, they appear in the table in this tab. To edit a configured profile, click **...**, and click its pencil icon. Edit the options in the window that pops up as described in the "DSP Farm Service Options" table, and click **Save Changes**. To delete a profile, click **...**, and click its trash can icon.

c) In **SCCP Config**, configure options as described in the SCCP options on page 77 topic.

8. Click **Save**.

A DSPFarm feature template is successfully added and configured.

What to do next

Proceed to add a voice policy if required for your Unified Communications deployment.

Media resource options

Describes available options for configuring media resources in a DSPFarm feature template, including selecting router resource modules and specifying their slot and sub-slot IDs, along with corresponding Cisco IOS CLI commands.

This reference topic describes the options available for configuring media resources within a DSPFarm feature template. These settings define the router resource modules that carry DSP resources and their physical placement (slot/sub-slot ID).

Table 31: Media Resource Options

Option	Description	Cisco IOS CLI Equivalent
Module	Select the router resource module to carry DSP resources that are used by DSPFarm profiles.	–
Slot/sub-slot ID	Select the slot and sub-slot in which the resource module that you selected resides.	**voice-card** *slot*/*subslot* **dsp service dspfarm**

DSPFarm service options

Details the configuration options for DSP farm services in a DSPFarm feature template, including service type selection, codec lists, session and participant limits, MTP settings, application association, and profile management parameters.

This reference topic describes the options available for configuring DSP farm services within a DSPFarm feature template. These settings define the type of DSP farm service (Transcoder, Conference, or MTP), codecs, maximum participants/sessions, and other service-specific parameters.

Table 32: DSP Farm Service Options

Option	Description	Cisco IOS CLI Equivalent
Profile Type	Select the type of DSP farm service that this profile is for. Options are **Transcoder**, **Conference**, and **MTP**	**dspfarm profile** *profile-identifier* {**conference** | **mtp** | **transcode**}
Profile ID	A system-generated unique identifier for the profile.	–
Universal	Available if you select Transcoder for the Profile Type When this check box is unchecked, transcoding is allowed only between the G.711 codec and other codecs. When this check box is checked, transcoding is allowed between codecs of any type.	**dspfarm profile** *profile-identifier* **transcode** [**universal**]

Option	Description	Cisco IOS CLI Equivalent
List Codec	Select the codecs that are available for the DSP farm service that this profile defines. The following codecs are supported. For MTP profile types, you can select one option, or you can select **pass-through** and one other option. If you want to change a codec, unselect the current codec before selecting a new one. • For the Transcoder profile type: • g711alaw, g711ulaw, g729abr8, g729ar8, g729br8, g729r8, g722-64, ilbc, iSAC • For the Conference profile type: • g711alaw, g711ulaw,g722r-64, g729abr8, g729ar8, g729br8, g729r8 • For the MTP profile type for software MTP only: • g711ulaw, g711alaw, g722-64, g729abr8, g729ar8, g729br8, g729r8, ilbc, iSAC, pass-through • For the MTP profile type for hardware MTP only, or for hardware and software MTP: • g711ulaw, g711alaw, pass-through	**codec** *codec-name*
Conference Maximum Participants	Available if you select Conference for the Profile Type. Select the maximum number of parties that can participate in a conference bridge (**8**, **16**, or **32**).	**maximum conference-participants** *number*

Option	Description	Cisco IOS CLI Equivalent
Maximum Sessions	Available if you select Transcoder or Conference for the Profile Type. Enter the maximum number of sessions that this profile can support. This value depends on the maximum number sessions that can be configured with the DSP resources that are available on the router. These resources are based on the type of modules in the router. To determine these resources, you can use a DSP calculator.	**maximum sessions** *number*
MTP Type	Available if you select MTP for the Profile Type. Select the way in which the router performs minor MTP translations such as G.711alaw to G.711ulaw, and DTMF conversions. Options are: • **Hardware**–MTP translations and conversions are performed by the hardware DSP resources • **Software**–MTP translations and conversions are performed by the router CPU	**maximum session** {**hardware** | **software**}
MTP Maximum Hardware Sessions	Available if you select Hardware for the MTP type. Select the maximum number of hardware sessions that can be used for MTP translations and conversions. Maximum value: 4000	**maximum session hardware** *number*
MTP Maximum Software Sessions	Available if you select Software for the MTP type. Select the maximum number of CPU sessions that can be used for MTP translations and conversions. Maximum value: 6000	**maximum session software** *number*
Application	Select the type of application to which the DSP farm services that are provisioned on the device are associated.	**associate application sccp**
Shutdown	Enable this option to take this profile out of service.	**shutdown**

SCCP options

Details the SCCP configuration options within a DSPFarm template, including setting the local interface, adding CUCM servers and groups, assigning priority, associating media resources and profiles, and selecting switchback and switchover methods for SCCP registration and failover.

This reference topic describes the options available for configuring SCCP (Signaling Connection Control Part) within a DSPFarm feature template. These settings define the local interface for SCCP communication and the Cisco Unified Communications Manager servers and groups to which DSP farm profiles will register.

Table 33: SCCP Options

Option	Description	Cisco IOS CLI Equivalent
CUCM Tab		
Configure up to 12 Cisco Unified Communications Manager servers to which the profiles that you defined in the Profile tab register.		
Local Interface	Enter the local interface that DSP services that are associated with the SCCP application use to register with Cisco Unified Communications Manager. Enter the interface in this format: *interface-type|interface-numberport* where: • *interface-type*–Type of interface that the services use to register with Cisco Unified Communications Manager. The type can be a GigabitEthernet interface or a port channel interface. • *interface-number*–Interface number that the services use to register with Cisco Unified Communications Manager. • *port*–(Optional) Port on which the interface communicates with Cisco Unified Communications Manager. If you do not specify a port, the default value 2000 is used. For example: GigabitEthernet0/0/0.	**sccp local** *interface-type interface-number* [**port** *port-number*]

Option	Description	Cisco IOS CLI Equivalent
Server List - *x*	Designate a Cisco Unified Communications Manager server to which the profiles that you defined in the Profile tab register. In the first field, enter the IP address or DNS name of the Cisco Unified Communications Manager server. In the second field, enter a numerical identifier for the Cisco Unified Communications Manager server. Click the Plus Sign icon (+) to configure up to 11 additional servers. To remove a server, click its corresponding Minus Sign icon. (-).	**sccp ccm** {*ipv4-address* | *ipv6-address* | *dns*} **identifier** *identifier-number* **version 7.0+**

CUCM Groups Tab

This tab is available when at least one Cisco Unified Communications Manager server is configured in the Cisco Unified Communications Manager tab.

Configure a Cisco Unified Communications Manager group, which includes up to 4 Cisco Unified Communications Manager servers that control the DSP farm services that, in turn, are associated with the servers.

If any Cisco Unified Communications Manager groups are already configured, they appear in the table in this tab. To edit a configured Cisco Unified Communications Manager group, click its pencil icon in the Action column, edit the options in the window that pops up as described in the following rows, and click **Save Changes**. To delete a Cisco Unified Communications Manager group, click its trash can icon in the Action column.

Add New CUCM Group	Click to add a new Cisco Unified Communications Manager group.	**sccp ccm group** *group-id*

Option	Description	Cisco IOS CLI Equivalent
Server Groups Priority Order	Select the priority in which the Cisco Unified Communications Manager servers in this Cisco Unified Communications Manager group are used. To do so: 1. Click this field to display a list of the Cisco Unified Communications Manager servers that you configured on the Cisco Unified Communications Manager tab. 2. Select the server that you want to be the primary server. This server has the highest priority. 3. Click the field again and select the server that you want to be the redundant server with the next highest priority. Repeat this step to select other redundant servers. The servers appear in this field in priority order. To remove a server from the group, click its X icon. To change the priority order of servers, remove the servers and add them back in the desired order.	**associate ccm** *cisco-unified-communications-manager-id* **priority** *priority*

Option	Description	Cisco IOS CLI Equivalent
CUCM Media Resource Name Profile to be Associated	In the Cisco Unified Communications Manager Media Resource Name field, enter a unique name that is used to register a DSP farm profile to the Cisco Unified Communications Manager servers. The name must contain from 6 to 15 characters. Characters can be letter, numbers, slashes (/), hyphens (-), and underscores (_). Space characters are not allowed. In the corresponding Profile to be Associated field, select a DSP farm profile to be registered to this Cisco Unified Communications Manager group using the name that you entered. To select a profile, click this field to display a list of the profile IDs that were configured on the Profile tab, and click the ID of the profile that you want. To add another Cisco Unified Communications Manager media resource name and profile, click the plus sign (+). You can add up to 4 Cisco Unified Communications Manager media resources and profiles. To remove a Cisco Unified Communications Manager media resource name and profile, click its corresponding minus sign (-).	**associate ccm** *profile-identifier* **register** *device-name*

Option	Description	Cisco IOS CLI Equivalent
CUCM Switchback	Select the switchback method that the Cisco Unified Communications Manager servers in this Cisco Unified Communications Manager group use to switch back after a failover: • **graceful**–Switchback occurs after all active sessions terminate gracefully. • **guard**–Switchback occurs either when active sessions are terminated gracefully or when the guard timer expires, whichever happens first. • **immediate**–Performs the Cisco Unified Communications Manager switchback to the higher priority Cisco Unified Communications Manager immediately when the timer expires, whether there is an active connection or not. Default: **graceful**.	**switchback method** {**graceful** | **guard** [*timeout-guard-value*] | **immediate**}
CUCM Switchover	Select the switchover method that Cisco Unified Communications Manager servers in this Cisco Unified Communications Manager use group when failing over: • **graceful**–Switchback occurs after all active sessions terminate gracefully. • **immediate**–Switchover occurs immediately, whether there is an active connection or not. Default: **graceful**.	**switchover method** {**graceful** | **immediate**}

Add a voice policy

Guides you through creating a new voice policy and configuring subpolicies for voice ports, POTS dial peers, SIP dial peers, and Cisco Unified SRST phones to tailor call handling for different endpoint types.

A voice policy defines how the system augments and manipulates calls for various endpoint types. This supertask guides you through the process of creating a new voice policy and configuring its subpolicies for different communication endpoints.

Voice policies are crucial for tailoring call functionality for specific endpoints, including voice ports, POTS dial peers, SIP dial peers, and Cisco Unified SRST phone profiles.

Before you begin

Follow these steps to add a voice policy:

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Unified Communications**.
2. Click **Add Voice Policy**.
3. In **Voice Policy Name**, enter a name for the policy.
4. Configure the required subpolicies:
   a) Configure voice ports for a voice policy.

      Define how the system augments and manipulates calls for voice port endpoint types. See Configure voice ports for a voice policy on page 82.

   b) Configure POTS Dial Peers for a voice policy.

      Define how the system augments and manipulates calls for POTS dial peer endpoint types. See Configure POTS dial peers for a voice policy on page 97.

   c) Configure SIP Dial Peers for a voice policy.

      Define how the system augments and manipulates calls for SIP dial peer endpoint types. See Configure SIP Dial Peers for a voice policy on page 106.

   d) Configure SRST Phones for a voice policy.

      Define how the system augments and manipulates calls for Cisco Unified SRST phone endpoint types. See Configure SRST phones for a voice policy on page 117

5. Click **Save Policy**.

A voice policy is successfully added and configured with its respective subpolicies.

What to do next

Proceed to provision a device template for Unified Communications to apply this voice policy to your devices.

Configure voice ports for a voice policy

Configure voice ports for a voice policy

This task defines how the system augments and manipulates calls for the voice port endpoint type within a voice policy. It allows you to set up various call functionality options such as trunk groups, translation rules, and line parameters.

When configuring voice ports for a voice policy, you define specific call functionality options depending on the type of voice card you are using (FXO, FXS, PRI ISDN, or FXS DID). These settings ensure calls are handled correctly based on your network requirements.

Before you begin

You must be in the process of adding a new voice policy or editing an existing one within Cisco SD-WAN Manager.

Follow these steps to configure voice ports for a voice policy:

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Unified Communications**.
2. Click **Add Voice Policy**, and choose **Voice Ports**.
3. In **Voice Ports**, enter a name for the policy

   From the **Add Voice Ports Policy Profile** drop-down list, select **Create New**.

Alternatively, you can select **Copy from Existing** to reuse settings from an existing policy profile.

4. Select **FXO**, **FXS**, **PRI ISDN**, or **FXS DID** to specify the type of voice port that the policy is for.
5. Select the types of call functionality policy options that you want to configure from the list of options that displays, and click **Next**.

   Available options include **Trunk Group**, **Translation Profile**, **Station ID**, **Line Params**, **Tuning Params**, **Supervisory Disconnect**, and **DID Timers**
6. Configure the selected call functionality options on the tabs that display: a.
   a) For **Trunk Group** options, configure settings as described in the Voice Ports Trunk Group Options topic.

      Define how voice ports function as members of a trunk group. After saving, configure priority by double-clicking the Priority field (1-64). If any trunk groups are already configured, they appear in the table. To edit, click **...** and select its pencil icon; to delete, select its trash can icon.

   b) For **Translation Profile** options, configure settings as described in the Voice ports translation profile options on page 87 topic.

      Define translation rules for calling and called numbers. After saving, double-click the dash (**-**) in the **Direction** column to select **Incoming** or **Outgoing**. You can create up to two translation profiles for this endpoint.

      You can create up to two translation profiles for this endpoint.

   c) For **Station ID** options, configure settings as described in the Voice ports station ID options on page 91 topic.

      Define the name and number for caller ID display.

   d) For **Line Params** options, configure settings as described in the Voice ports line parameters options on page 91 topic.

      Define line parameters for voice quality.

   e) For **Tuning Params** options, configure settings as described in the Voice Ports Tuning Parameters Options topic.

      Define parameters for signaling between voice ports and other instruments.

   f) For **Supervisory Disconnect** options, configure settings as described in the Voice ports supervisory disconnect options on page 94 topic.

      Define parameters for supervisory disconnect events. You can configure as many supervisory disconnect events as needed.

   g) For **DID Timers** options, configure settings as described in the Voice ports DID timers options on page 96 topic.

      Define timers for Direct Inward Dialing (DID) calls.
7. Click **Next**.
8. In **Policy Profile Name**, enter a name for this child policy.
9. In **Policy Profile Description**, enter a description for this child policy.
10. Click **Save**.

The voice ports for the voice policy are successfully configured.

What to do next

Return to the main Add a Voice Policy supertask to continue configuring other subpolicies (POTS Dial Peers, SIP Dial Peers, SRST Phones) as needed.

Voice ports trunk group options

Voice ports trunk group options

This reference topic describes the options available for configuring trunk groups for voice ports within a voice policy. These settings define how voice ports function as members of a trunk group, including hunt schemes and call limits.

Table 34: Trunk group options

Option	Description	Cisco IOS CLI Equivalent
Add New Trunk Group	Click to add a trunk group for the selected card. You can add one trunk group for a voice port.	–
Copy from Existing	Click to copy an existing trunk group to a new trunk group. In the box that appears, change the name if desired, select a trunk group, and click **Copy**.	–
Name	Name of the trunk group. The name can contain up to 32 characters.	**trunk group** *name*

Option	Description	Cisco IOS CLI Equivalent
Hunt-Scheme		**trunk group** *name* **hunt-scheme least-idle [both | even | odd]** **hunt-scheme least-used [both | even | odd]** **hunt-scheme longest-idle [both | even | odd]** **hunt-scheme round-robin [both | even | odd]** **hunt-scheme sequential [both | even | odd]** **hunt-scheme random**

Option	Description	Cisco IOS CLI Equivalent
	Select the hunt scheme in the trunk group for outgoing calls: • **least-idle both**–Searches for an idle channel with the shortest idle time • **least-idle even**–Searches for an idle even-numbered channel with the shortest idle time • **least-idle odd**–Searches for an idle odd-numbered channel with the shortest idle time • **least-used both**–Searches for a trunk group member that has the highest number of available channels (applies only to PRI ISDN cards) • **least-used even**–Searches for a trunk group member that has the highest number of available even-numbered channels (applies only to PRI ISDN cards) • **least-used odd**–Searches for a trunk group member that has the highest number of available odd-numbered channels (applies only to PRI ISDN cards) • **longest-idle both**–Searches for an idle odd-numbered channel with the longest idle time • **longest-idle even**–Searches for an idle channel that has the highest number of available even-numbered channels • **longest-idle odd**–Searches for an idle channel that has the highest number of available odd-numbered channels • **round-robin both**–Searches trunk group members in turn for an idle channel, starting with the trunk group member that follows the last used member • **round-robin even**–Searches trunk group member in turn for an idle even-numbered channel, starting with the trunk group member that follows the last used member • **round-robin odd**–Searches trunk group member in turn for an idle odd-numbered channel, starting with the trunk group member that follows the last used member • **sequential-both**–Searches for an idle channel, starting with the trunk group member with the highest preference within the trunk	

Option	Description	Cisco IOS CLI Equivalent
	group • **sequential-even**–Searches for an idle even-numbered channel, starting with the trunk group member with the highest preference within the trunk group • **sequential-odd**–Searches for an idle odd-numbered channel, starting with the trunk group member with the highest preference within the trunk group • **random**–Searches for a trunk group member at random and selects a channel from the member at random Default: least-used both	
Max Calls	Enter the maximum number of calls that are allowed for the trunk group. If you do not enter a value, there is no limit on the number of calls. If the maximum number of calls is reached, the trunk group becomes unavailable for more calls. • In field–Enter the maximum number of incoming calls that are allowed for this trunk group • Out field– Enter the maximum number of outgoing calls that are allowed for this trunk group Valid range for both fields: integers 0 through 1000.	**trunk group** *name* **max-calls voice** *number-of-calls* **direction** [**in** | **out**]
Max-Retry	Select the maximum number of outgoing call attempts that the trunk group makes if an outgoing call fails. If you do not enter a value and a call fails, the system does not attempt to make the call again. Valid range: integers 1 through 5.	**trunk group** *name* **max-retry** *attempts*
Save Trunk Group	Click to save the Trunk Group that you configured.	–

Voice ports translation profile options

translation profile options

This reference topic describes the options available for configuring translation profiles for calling and called numbers for voice ports within a voice policy. These settings allow you to define rules for matching and replacing number strings.

Table 35: Translation profile options

Option	Description	Cisco IOS CLI Equivalent
Add New Translation Profile	Click to add a translation profile for the selected card. You can create up to two translation profiles for this endpoint.	**voice translation-profile** *name*
Copy from Existing	Click to copy an existing translation profile to a new translation profile. In the box that appears, change the name if desired, select a called translation rule and a calling translation rule, and click **Copy**.	–
Calling	Click to configure translation rules for the number that is calling in. The Translation Rules pane displays.	**translate calling** *translation-rule-number*
Called	Click to configure translation rules for the number that is being called. The Translation Rules pane displays.	**translate called** *translation-rule-number*

Option	Description	Cisco IOS CLI Equivalent
Translation Rules pane		**voice translation-rule** *number* Match and Replace Rule: **rule** *precedence* /*match-pattern*/ / *replace-pattern*/ Reject Rule: **rule** *precedence* **reject** /*match-pattern*/

Option	Description	Cisco IOS CLI Equivalent
	1. Click **Add New** to create a translation rule. Alternatively, you can click **Copy From Existing** to copy an existing translation rule to a new translation rule. In the box that appears, change the name if desired, select a called translation rule and a calling translation rule, and click **Copy**. 2. In the Translation Rule Number field, enter a unique number that designates the precedence for this rule. Valid range: integers 1 through 100. 3. (Optional) To copy existing translation rules from a CSV file, click **Import**. Continue to add rules or click **Finish**. For detailed information about this file, see Translation rules CSV file on page 122. 4. Click **Add Rule**. 5. In the Match field, enter the string that you want the translation rule to affect. Enter the string in regular expression format beginning and ending with a slash (/). For example, /^9/. To include the backslash character (\) in a match string, precede the backslash with a backslash. 6. From the Action drop-down list, select the action that the system performs for calls that match the string in the Match field. The **Reject** option causes the system to reject the call. The **Replace** option causes the system to replace the match number with a value that you specify. 7. If you select the **Replace** action, in the Replace field that displays, enter the string to which to translate the matched string. Enter the number in regular expression format beginning and ending with a slash (/). For example, //, which indicates a replacement of no string. To include the backslash character (\) in a replace string, precede the backslash with a backslash. As an example, if you specify a match string of /^9/ and a replace string of //, the system removes the leading 9 from calls with a number that begins with 9. In this case, the system translates 914085551212 to 14085551212. 8. Click **Save**.	

Option	Description	Cisco IOS CLI Equivalent
	9. Add more translation rules as needed. 10. (Optional) Click **Export** to save the translation rules that you created in a CSV file. 11. Click **Finish** at the bottom of the pane.	

Voice ports station ID options

Voice ports station ID options

This reference topic describes the options available for configuring station ID information for voice ports within a voice policy. These settings define the name and number displayed for caller ID.

Table 36: Station ID Options

Option	Description	Cisco IOS CLI Equivalent
Station Name	Enter the name of the station. The station name can contain up to 50 letters, numbers, and spaces, dashes (-), and underscores (_).	**station-id name** *name*
Station Number	Enter the phone number of the station in E.164 format. The station number can contain up to 15 numeric characters.	**station-id number** *number*

Voice ports line parameters options

Voice ports line parameters options

This reference topic describes the options available for configuring line parameters for voice ports within a voice policy. These settings control voice quality aspects such as gain, attenuation, echo cancellation, and companding type.

Table 37: Line Parameters Options

Option	Description	Cisco IOS CLI Equivalent
Gain	Enter the gain, in dB, for voice input. Valid range: -6 through 14. Default: 0	**input gain** *decibels*
Attenuation	Enter the amount of attenuation, in dB, for transmitted voice output. Valid range: -6 through 14. Default: 3.	**output attenuation** *decibels*
Echo Canceller	Select **Enable** to apply echo cancellation to voice traffic. By default, this option is enabled.	**echo-cancel** *enable*
Voice Activity Detection (VAD)	Select **Enable** to apply VAD to voice traffic. By default, this option is enabled.	**vad**

Option	Description	Cisco IOS CLI Equivalent
Compand Type	Select the companding standard to be used to convert between analog and digital signals in PCM systems (**U-law** or **A-law**). Default: U-Law.	**compand-type {u-law | a-law}**
Impedance	This field does not apply to PRI ISDN cards. Select the terminating impedance for calls. Default: 600r.	**impedance {600c | 600r 900c | 900r | complex1 | complex2 | complex3 | complex4 | complex5 | complex6}**
Call Progress Tone	Select the locale for call progress tones.	**cptone** *locale*

Voice ports tuning parameters options

Voice ports tuning parameters options

This reference topic describes the options available for configuring tuning parameters for voice ports within a voice policy. These settings define signaling parameters between voice ports and other instruments, with specific options for FXO and FXS cards.

Table 38: Tuning Parameters Options

Option	Description	Cisco IOS CLI Equivalent
Tuning Params Options for FXO Cards		
Pre Dial Delay	Enter the delay, in seconds, of the delay on the FXO interface between the beginning of the off-hook state and the initiation of DTMF signaling. Valid range: 0 through 10. Default: 1.	**pre-dial-delay** *seconds*
Supervisory Disconnect	Select the type of tone that indicates that a call has been released and that a connection should be disconnected: • **Anytone**–Any tone indicates a supervisory disconnect • **Signal**–A disconnect signal indicates a supervisory disconnect • **Dualtone**–A dual-tone indicates a supervisory disconnect Default: Signal.	Anytone: supervisory disconnect **anytone** Signal: supervisory disconnect Dualtone: supervisory disconnect **dualtone {mid-call | pre-connect}**
Dial Type	Select the dialing method for outgoing calls: • **pulse**–Pulse dialer • **dtmf**–Dual-tone multifrequency dialer • **mf**–Multifrequency dialer Default: dtmf.	**dial-type {dtmf | pulse | mf}**

Option	Description	Cisco IOS CLI Equivalent
Timing Sup-Disconnect	Enter the minimum time, in milliseconds, that is required to ensure that an on-hook indication is intentional and not an electrical transient on the line before a supervisory disconnect occurs (based on power denial signaled by the PSTN or PBX). Valid range: 50 through 1500. Default: 350.	**timing sup-disconnect** *milliseconds*
Battery Reversal	Battery reversal reverses the battery polarity on a PBX when a call connects, then changes the battery polarity back to normal when the far-end disconnects. Select **Answer** to configure the port to support answer supervision by detection of battery reversal. Select **Detection Delay** to configure the delay time after which the card acknowledges a battery-reversal signal, then enter the delay time in milliseconds. Valid range: 0 through 800. Default: 0 (no delay). If an FXO port or its peer FXS port does not support battery reversal, do not configure battery reversal options to avoid unpredictable behavior.	**battery-reversal** [**answer**] **battery-reversal-detection-delay** *milliseconds*
Timing Hookflash out	Enter the duration, in milliseconds, of hookflash indications that the gateway generates on the FXO interface. Valid range: 50 through 1550. Default: 400.	**timing hookflash-out** *milliseconds*
Timing Guard out	Enter the number of milliseconds after a call disconnects before another outgoing call is allowed. Valid range: 300 through 3000. Default: 2000.	**timing guard-out** *milliseconds*
Tuning Params Options for FXS Cards		
Timing Hookflash In	Enter the minimum and maximum duration, in milliseconds, of an on-hook condition to be interpreted as a hookflash by the FXS card. Valid range for minimum duration: 0 through 400. Default minimum value: 50. Valid range for maximum duration: 50 through 1500. Default maximum value: 1000.	**timing hookflash-in** *maximum-milliseconds minimum-milliseconds*
Pulse Digit Detection	To enable pulse digit detection at the beginning of a call, select **Yes**. Default: Yes.	**pulse-digit-detection**
Loop Length	Select the length for signaling on FXS ports (**Long** or **Short**). Default: Short.	**loop-length** [**long** | **short**]

Option	Description	Cisco IOS CLI Equivalent
Ring	• **Frequency**–Select the frequency, in Hz, of the alternating current that, when applied, rings a connected device. Default: 25. • **DC Offset**–Applies only if Loop Length is set to Long. Select the voltage threshold below which a ring does not sound on devices. Valid values: 10-volts, 20-volts, 24-volts, 30-volts, and 35-volts.	**ring frequency** *number* **ring dc-offset** *number*
Ringer Equivalence Number (REN)	Select the REN for calls that this card processes. This number specifies the loading effect of a telephone ringer on a line. Valid range: 1 through 5. Default: 1.	**ren** *number*

Voice ports supervisory disconnect options

Details the configurable options for supervisory disconnect events on voice ports, including mode selection, cptone and dual-tone detection parameters, cadence, frequency settings, and related Cisco IOS CLI commands to define call disconnection behavior, especially for FXO cards.

This reference topic describes the options available for configuring supervisory disconnect events for voice ports within a voice policy. These settings define how the system detects and handles call disconnections, particularly for FXO cards.

Table 39: Supervisory Disconnect Options

Option	Description	Cisco IOS CLI Equivalent
Add New Supervisory Disconnect	Click to add a supervisory disconnect event.	–
Mode	Choose the mode for the supervisory disconnect event: • **Custom CPTone**–Provides options for configuring cptone detection parameters for a supervisory disconnect event • **Dual Tone Detection Params**– Provides options for configuring dual-tone detection parameters for a supervisory disconnect event	**voice class custom-cptone** *cptone-name* **voice class dualtone-detect-params** *tag*
Supervisory Name	Applies to Custom CPTone mode. Enter a name for the supervisory disconnect event. The name can contain up to 32 characters. Valid characters are letters, numbers, dashes (-), and underscores (_).	**voice class custom-cptone** *cptone-name*

Option	Description	Cisco IOS CLI Equivalent
Dualtone	Applies to Custom CPTone mode. Select the type of dual-tone that causes a disconnect. Options are: • Busy • Disconnect • Number Unobtainable • Out of Service • Reorder • Ringback	**dualtone** {**ringback** |**busy** | **reorder** | **out-of-service** | **number-unobtainable** | **disconnect**}
Cadence	Applies to Custom CPTone mode. Enter the cadence interval, in milliseconds, of the dual-tones that cause a disconnect. Enter the cadence as an on/off value pair, separated with a space. You can enter up to 4 on/off value pairs, separated with a space.	**cadence** *cycle-1-on-time cycle-1-off-time* [*cycle-2-on-time cycle-2-off-time* [*cycle-3-on-time cycle-3-off-time* [*cycle-4-on-time cycle-4-off-time*]]]
Dualtone Frequency	Applies to Custom CPTone mode. Enter the frequency, in Hz, of each tone in the dual-tone. Valid range for each tone is 300 through 3600.	**frequency** *frequency-1* [*frequency-2*]
Supervisory Number	Applies to Custom Dual Tone Detection Params mode. Enter a unique number to identify dual-tone detection parameters. Valid range: 1 through 10000.	**voice class dualtone-detect-params** *tag-number*
Cadence-Variation	Applies to Custom Dual Tone Detection Params mode. Enter the maximum time, in milliseconds, by which the tone onset can vary from the onset time and still be detected. The system multiplies the value that you enter by 10. Valid range: 0 through 200 in units of 10. Default: 10.	**cadence-variation** *time*

Option	Description	Cisco IOS CLI Equivalent
Frequency	Applies to Custom Dual Tone Detection Params mode. • Max Delay–Enter the maximum delay, in milliseconds, before a supervisory disconnect is performed after the dual-tone is detected. The system multiplies the value that you enter by 10. Valid range: 0 through 100 in units of 10. Default: 10. • Max Deviation–Enter the maximum deviation, in Hz, by which each tone can deviate from configured frequencies and be detected. Valid range: 10 through 125. Default: 10. • Max Power–Enter the power of the dual-tone, in dBm0, above which a supervisory disconnect is no detected. Valid range: 0 through 20. Default: 10. • Min Power– Enter the power of the dual-tone, in dBm0, below which a supervisory disconnect is not detected. Valid range: 10 through 35. Default: 30. • Power Twist–Enter difference, in dBm0, between the minimum power and the maximum power of the dual-tone above which a supervisory disconnect is not detected. Valid range: 0 through 15. Default: 6.	**freq-max-delay** *time* **freq-max-deviation** *hertz* **freq-max-power** *dBm0* **freq-min-power** *dBm0* **freq-power-twist** *dBm0*
Save	Click to save the supervisory disconnect information that you configured.	–

Voice ports DID timers options

Details the available options for configuring DID timers on voice ports, including parameters such as wait before wink, wink duration, clear wait, dial pulse min delay, and answer winkwidth, along with their Cisco IOS CLI equivalents.

This reference topic describes the options available for configuring DID (Direct Inward Dialing) timers for voice ports within a voice policy.

Table 40: DID Timers Options

Option	Description	Cisco IOS CLI Equivalent
Wait Before Wink	Enter the amount of time, in milliseconds, that the card waits after receiving a call before sending a wink signal to notify the remote side that it can send DNIS information. Valid range: 100 through 6500. Default: 550.	**timing wait-wink** *milliseconds*

Option	Description	Cisco IOS CLI Equivalent
Wink Duration	Enter the maximum amount of time, in milliseconds, of the wink signal for the card. Valid range: 50 through 3000. Default: 200.	**timing wait-duration** *milliseconds*
Clear Wait	Enter the minimum amount of time, in milliseconds, between an inactive seizure signal and the call being cleared for the card. Valid range: 200 through 2000. Default: 400.	**timing clear-wait** *milliseconds*
Dial Pulse Min Delay	Enter the amount of time, in milliseconds, between wink-like pulses for the card. Valid range: 0 or 140 through 5000. Default: 140.	**timing dial-pulse min-delay** *milliseconds*
Answer Winkwidth	Enter the minimum delay time, in milliseconds, between the start of an incoming seizure and the wink signal. Valid range: 110 through 290. Default: 210.	**timing answer-winkwidth** *milliseconds*

Configure POTS dial peers for a voice policy

Configure POTS Dial Peers for a voice policy

This task defines how the system augments and manipulates calls for the POTS dial peer endpoint type within a voice policy. It allows you to configure options such as trunk groups and translation profiles to manage call flow.

When configuring POTS dial peers for a voice policy, you define specific options that control how the system handles calls for this endpoint type. This includes settings for how calls are routed through trunk groups and how calling/called numbers are translated. Trunk Group configuration for POTS Dial Peers is available beginning with Cisco IOS XE Catalyst SD-WAN Release 17.3.1a.

Before you begin

You must be in the process of adding a new voice policy or editing an existing one within Cisco SD-WAN Manager.

Follow these steps to configure POTS dial peers for a voice policy:

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Unified Communications**
2. Click **Add Voice Policy**, and choose **POTS Dial Peer** in the left pane.
3. From the **Add POTS Dial Peer Policy Profile** drop-down list, select **Create New**.

   Alternatively, you can select **Copy from Existing** to reuse settings from an existing policy profile.
4. Select the types of POTS dial peers that you that you want to configure from the list of options that displays, and click **Next**.

   Options include **Trunk Group** (beginning with Cisco IOS XE Catalyst SD-WAN Release 17.3.1a) and **Translation Profile**.
5. Configure the selected POTS dial peer options:
   a) To configure trunk groups, configure options as described in the Voice policy POTS dial peer trunk group options on page 98 topic.

Define how POTS dial peers function within trunk groups.

You can create up to 64 trunk groups for this endpoint. If any trunk groups are already configured, they appear in the trunk groups table on this page. To edit, click **...**, and select its pencil icon; to delete, select its trash can icon. After saving, configure the priority for a trunk group by double-clicking the Priority field (1-64) and entering a number. The number you enter is the priority of the POTS dial peer in the trunk group for incoming and outgoing calls.

b) To configure translation profiles, configure options as described in the Voice policy POTS dial peer translation profile options on page 102 topic.

Define translation rules for calling and called numbers.

You can create up to two translation profiles for this endpoint. After saving, double-click the dash (-) in the **Direction** column to select **Incoming** or **Outgoing**.

The **Incoming** selection applies the corresponding translation rule to traffic that is incoming to this endpoint. The **Outgoing** selection applies the corresponding translation rule to traffic that is outgoing from this endpoint.

6. Click **Next**.
7. In **Policy Profile Name**, enter a name for this child policy.
8. In **Policy Profile Name**, enter a name for this child policy.
9. In **Policy Profile Description**, enter a description for this child policy.
10. Click **Save**.

The POTS dial peers for the voice policy are successfully configured.

What to do next

Return to the main Add a Voice Policy supertask to continue configuring other subpolicies (SIP Dial Peers, SRST Phones) as needed.

Voice policy POTS dial peer trunk group options

Voice policy POTS dial peer trunk group options

This reference topic describes the options available for configuring trunk groups for POTS dial peers within a voice policy. These settings define how POTS dial peers are organized into trunk groups, including hunt schemes and maximum call limits.

Table 41: POTS dial peer trunk group options

Option	Description	Cisco IOS CLI Equivalent
Add New Trunk Group	Click to add a trunk group for the selected card. You can add one trunk group for a voice port.	–

Option	Description	Cisco IOS CLI Equivalent
Copy from Existing	Click to copy an existing trunk group to a new trunk group. In the box that appears, change the name if desired, select a trunk group, and click **Copy**. A trunk group name whose name is preceded with "{Master}" is already associated with this voice policy. When you copy a this type of trunk group, the system reuses the existing trunk group without creating another instance of the trunk group definition. In this case, you cannot change the name.	–
Name	Name of the trunk group. The name can contain up to 32 characters.	**trunk group** *name*

Option	Description	Cisco IOS CLI Equivalent
Hunt-Scheme		**trunk group** *name* **hunt-scheme least-idle [both | even | odd]** **hunt-scheme least-used [both | even | odd]** **hunt-scheme longest-idle [both | even | odd]** **hunt-scheme round-robin [both | even | odd]** **hunt-scheme sequential [both | even | odd]** **hunt-scheme random**

Option	Description	Cisco IOS CLI Equivalent
	Select the hunt scheme in the trunk group for outgoing calls: • **least-idle both**–Searches for an idle channel with the shortest idle time • **least-idle even**–Searches for an idle even-numbered channel with the shortest idle time • **least-idle odd**–Searches for an idle odd-numbered channel with the shortest idle time • **least-used both**–Searches for a trunk group member that has the highest number of available channels (applies to only PRI ISDN cards) • **least-used even**–Searches for a trunk group member that has the highest number of available even-numbered channels (applies only to PRI ISDN cards) • **least-used odd**–Searches for a trunk group member that has the highest number of available odd-numbered channels (applies only to PRI ISDN cards) • **longest-idle both**–Searches for an idle odd-numbered channel with the longest idle time • **longest-idle even**–Searches for an idle channel that has the highest number of available even-numbered channels • **longest-idle odd**–Searches for an idle channel that has the highest number of available odd-numbered channels • **round-robin both**–Searches trunk group members in turn for an idle channel, starting with the trunk group member that follows the last used member • **round-robin even**–Searches trunk group member in turn for an idle even-numbered channel, starting with the trunk group member that follows the last used member • **round-robin odd**–Searches trunk group member in turn for an idle odd-numbered channel, starting with the trunk group member that follows the last used member • **sequential-both**–Searches for an idle channel, starting with the trunk group member with the highest preference within the trunk	

Option	Description	Cisco IOS CLI Equivalent
	group • **sequential-even**–Searches for an idle even-numbered channel, starting with the trunk group member with the highest preference within the trunk group • **sequential-odd**–Searches for an idle odd-numbered channel, starting with the trunk group member with the highest preference within the trunk group • **random**–Searches for a trunk group member at random and selects a channel from the member at random Default: **least-used both**	
Max Calls	Enter the maximum number of calls that are allowed for the trunk group. If you do not enter a value, there is no limit on the number of calls. If the maximum number of calls is reached, the trunk group becomes unavailable for more calls. • **In field**–Enter the maximum number of incoming calls that are allowed for this trunk group. • **Out field**– Enter the maximum number of outgoing calls that are allowed for this trunk group. Valid range for both fields: integers 0 through 1000.	**trunk group** *name* **max-calls voice** *number-of-calls* **direction** [**in** | **out**]
Max-Retry	Select the maximum number of outgoing call attempts that the trunk group makes if an outgoing call fails. If you do not enter a value and a call fails, the system does not attempt to make the call again. Valid range: integers 1 through 5.	**trunk group** *name* **max-retry** *attempts*

Voice policy POTS dial peer translation profile options

Voice policy POTS dial peer translation profile options

This reference topic describes the options available for configuring translation profiles for POTS dial peers within a voice policy. These settings allow you to define rules for matching and replacing calling and called number strings for POTS dial peer calls.

Table 42: POTS dial peer translation profile options

Option	Description	Cisco IOS CLI Equivalent
Add New Translation Profile	Click to add a translation profile for the selected POTS dial peer. You can create up to two translation profiles for this endpoint.	–
Copy from Existing	Click to copy an existing translation profile to a new translation profile. In the box that appears, change the name if desired, select a called translation rule and a calling translation rule, and click **Copy**.	–
Name	Name of the translation profile. The name can contain up to 32 characters.	**voice translation-profile** *name*
Calling	Click to configure translation rules for the number that is calling in. The Translation Rules pane displays.	**translate calling** *translation-rule-number*
Called	Click to configure translation rules for the number that is being called. The Translation Rules pane displays.	**translate called** *translation-rule-number*

Option	Description	Cisco IOS CLI Equivalent
Translation Rules pane		**voice translation-rule** *number* Match and Replace Rule: **rule** *precedence* /*match-pattern*/ / *replace-pattern*/ Reject Rule: **rule** *precedence* **reject** /*match-pattern*/

Option	Description	Cisco IOS CLI Equivalent
	1. Click **Add New** to create a translation rule. Alternatively, you can click **Copy From Existing** to copy an existing translation rule to a new translation rule. In the box that appears, change the name if desired, select a called translation rule and a calling translation rule, and click **Copy**. 2. In the Translation Rule Number field, enter a unique number that designates the precedence for this rule. Valid range: integers 1 through 100. 3. (Optional) To copy existing translation rules from a CSV file, click **Import**. Continue to add rules or click **Finish**. For detailed information about this file, see Translation rules CSV file on page 122. 4. Click **Add Rule**. 5. In the Match field, enter the string that you want the translation rule to affect. Enter the string in regular expression format beginning and ending with a slash (/). For example, /^9/. To include the backslash character (\) in a match string, precede the backslash with a backslash. 6. From the **Action** drop-down list, select the action that the system performs for calls that match the string in the Match field. The **Reject** option causes the system to reject the call. The **Replace** option causes the system to replace the match number with a value that you specify. 7. If you select the **Replace** action, in the Replace field that displays, enter the string to which to translate the matched string. Enter the number in regular expression format beginning and ending with a slash (/). For example, //, which indicates a replacement of no string. To include the backslash character (\) in a replace string, precede the backslash with a backslash. As an example, if you specify a match string of /^9/ and a replace string of //, the system removes the leading 9 from calls with a number that begins with 9. In this case, the system translates 914085551212 to 14085551212. 8. Click **Save**.	

Option	Description	Cisco IOS CLI Equivalent
	9. Add more translation rules as needed. 10. (Optional) Click **Export** to save the translation rules that you created in a CSV file. 11. Click **Finish** at the bottom of the pane.	

Configure SIP Dial Peers for a voice policy

Configure SIP Dial Peers for a voice policy

This task defines how the system augments and manipulates calls for the SIP dial peer endpoint type within a voice policy. It allows you to configure options such as translation profiles, media profiles, modem pass-through, and fax protocols.

When configuring SIP dial peers for a voice policy, you define specific options that control how the system handles calls for this endpoint type. This includes settings for how calling/called numbers are translated, codec preferences, DTMF relay options, and fax capabilities.

Before you begin

You must be in the process of adding a new voice policy or editing an existing one within Cisco SD-WAN Manager.

Follow these steps to configure SIP dial peers for a voice policy:

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Unified Communications**.
2. Click **SIP Dial Peer**.
3. From the **Add SIP Dial Peer Policy Profile** drop-down list, choose **Create New**.

   Alternatively, you can select **Copy from Existing** to reuse settings from an existing policy profile.
4. Select the policy types that you want to create and click **Next**.
5. In the page that displays, configure options in the tabs as needed:
   a) For Translation Profile options, configure settings as described in the Voice policy SIP dial peer translation profile options on page 107 topic.

      Define translation rules for calling and called numbers.

      After you click **Finish** when configuring a translation profile, you can add another translation profile (up to two for this endpoint). Click **Save Translation Profile**. For each translation profile, double-click the dash (-) in the **Direction** column to select **Incoming** or **Outgoing**.

   b) For Media Profile options, configure settings as described in the Voice policy SIP Dial Peer Media profile options on page 110 topic.

      Define codecs and DTMF relay options for SIP calls.

   c) For Modem Pass-through options, configure settings as described in the Voice Policy SIP Dial Peer Modem Pass-Through Options topic.

      Configure the modem pass-through feature for this endpoint.

   d) For Fax Protocol options, configure settings as described in the Voice policy SIP dial peer fax protocol options on page 111 topic.

      Configure the fax protocol capability for this endpoint.

6. Click **Next**.
7. In **Policy Profile Name**, enter a name for this child policy.
8. In **Policy Profile Description**, enter a description for this child policy.
9. Click **Save**.

The SIP dial peers for the voice policy are successfully configured.

What to do next

Return to the main Add a Voice Policy supertask to continue configuring other subpolicies (SRST Phones) as needed.

Voice policy SIP dial peer translation profile options

Voice policy SIP dial peer translation profile options

This reference topic describes the options available for configuring translation rules for calling and called numbers for SIP dial peers within a voice policy. These settings allow you to define rules for matching and replacing number strings for SIP dial peer calls.

Table 43: Voice policy SIP dial peer translation profile options

Option	Description	Cisco IOS CLI Equivalent
Add New Translation Profile	Click to add a translation profile for the selected SIP dial peer. You can create up to two translation profiles for this endpoint.	**voice translation-profile** *name*
Copy from Existing	Click to copy an existing translation profile to a new translation profile. In the box that appears, change the name if desired, select a called translation rule and a calling translation rule, and click **Copy**.	–
Calling	Click to configure translation rules for the number that is calling in. The Translation Rules pane displays.	**translate calling** *translation-rule-number*
Called	Click to configure translation rules for the number that is being called. The Translation Rules pane displays.	**translate called** *translation-rule-number*

Option	Description	Cisco IOS CLI Equivalent
Translation Rules pane		**voice translation-rule** *number* Match and Replace Rule: **rule** *precedence* /*match-pattern*/ / *replace-pattern*/ Reject Rule: **rule** *precedence* **reject** /*match-pattern*/

Option	Description	Cisco IOS CLI Equivalent
	1. Click **Add New** to create a translation rule. Alternatively, you can click **Copy From Existing** to copy an existing translation rule to a new translation rule. In the box that appears, change the name if desired, select a called translation rule and a calling translation rule, and click **Copy**. 2. In the Translation Rule Number field, enter a unique number that designates the precedence for this rule. Valid range: integers 1 through 100. 3. (Optional) To copy existing translation rules from a CSV file, click **Import**. Continue to add rules or click **Finish**. For detailed information about this file, see Translation rules CSV file on page 122. 4. Click **Add Rule**. 5. In the Match field, enter the string that you want the translation rule to affect. Enter the string in regular expression format beginning and ending with a slash (/). For example, /^9/. To include the backslash character (\) in a match string, precede the backslash with a backslash. 6. From the Action drop-down list, select the action that the system performs for calls that match the string in the Match field. The **Reject** option causes the system to reject the call. The **Replace** option causes the system to replace the match number with a value that you specify. 7. If you select the **Replace** action, in the Replace field that displays, enter the string to which to translate the matched string. Enter the number in regular expression format beginning and ending with a slash (/). For example, //, which indicates a replacement of no string. To include the backslash character (\) in a replace string, precede the backslash with a backslash. As an example, if you specify a match string of /^9/ and a replace string of //, the system removes the leading 9 from calls with a number that begins with 9. In this case, the system translates 914085551212 to 14085551212. 8. Click **Save**.	

Option	Description	Cisco IOS CLI Equivalent
	9. Add more translation rules as needed. 10. (Optional) Click **Export** to save the translation rules that you created in a CSV file. 11. Click **Finish** at the bottom of the pane.	

Voice policy SIP Dial Peer Media profile options

Voice policy SIP dial peer media profile options

This reference topic describes the options available for configuring media profiles for SIP dial peers within a voice policy. These settings define the codecs available for SIP trunk communication and DTMF relay options for SIP calls.

Table 44: Voice policy SIP dial peer media profile options

Option	Description	Cisco IOS CLI Equivalent
Add New Media Profile	Click to add a translation profile for the dial peer.	–
Copy from Existing	Click to copy an existing media profile to a new media profile. In the box that appears, enter a media profile number for the profile, and click **Copy**.	–
Media Profile Number	Enter a number for this SIP media profile. Valid range: Integers 1 through 10000.	**voice class codec** *tag-number*
Codec	Move from the Source list to the Target list the codecs that you want to be made available for the SIP trunk to use when communicating with the remote dial peer. Codecs in the target list are in descending order of priority, with the highest priority at the top of the list. Drag and drop items in this list to rearrange them.	**voice class codec** *tag-number* **codec preference** *value codec-type*
DTMF	Move from the Source list to the Target list the DTMF relay options that you want the system to use for SIP calls. Items in the Target list are in descending order of priority, with the highest priority at the top of the list. Drag and drop items in this list to rearrange them. If you want to include the **Inband** option in the Target list, it can be the only option in that list. If you want to include other options in the Target list, move the Inband option to the Source list before saving the media profile.	**dtmf-relay** {[[**sip-notify**] [**sip-kpml**] [**rtp-nte**]]}
Save	Click to save the configuration settings that you made.	–

Voice policy SIP dial peer modem pass-through options

Voice policy SIP dial peer modem pass-through options

This reference topic describes the options available for configuring modem pass-through features for SIP dial peers within a voice policy. These settings define the protocol for modem pass-through functionality.

Table 45: Voice policy SIP dial peer modem pass-through options

Option	Description	Cisco IOS CLI Equivalent
Add New Modem Pass-through	Click to add a modem pass-through for this SIP dial peer endpoint.	–
Copy from Existing	Click to copy an existing modem pass-through to a new modem pass-through profile. In the box that appears, select an existing modem pass-through, enter new name if desired, and click **Copy**.	–
Name	Name of the modem pass-through. This name is used when you copy an existing modem pass-through profile to a new one.	–
Protocol	Select the protocol for the modem pass-through: • **None**–Modem pass-through is disabled on the device • **NSE G.711ulaw**–Uses named signaling events (NSEs) to communicate G.711ulaw codec switchover between gateways • **NSE G.711alaw**–Uses named signaling events (NSEs) to communicate G.711alaw codec switchover between gateways	None: **no modem passthrough** NSE G.711 ulaw: **modem passthrough nse codec g711ulaw** NSE G.711 alaw: **modem passthrough nse codec g711alaw**
Save Modem Pass-Through	Click to save the configuration settings that you made.	–

Voice policy SIP dial peer fax protocol options

Outlines the configuration options for fax protocols on SIP dial peers within a voice policy, including primary and fallback protocol selection, T.38 fax relay and pass-through modes, speed and redundancy settings, ECM management, and relevant Cisco IOS CLI equivalents.

This reference topic describes the options available for configuring fax protocol capabilities for SIP dial peers within a voice policy. These settings define the primary and fallback fax protocols, including various T.38 fax relay and pass-through options.

Table 46: Voice policy SIP dial peer fax protocol options

Option	Description	Cisco IOS CLI Equivalent
Add New Fax Protocol	Click to add a fax protocol for the dial peer.	–

Option	Description	Cisco IOS CLI Equivalent
Copy from Existing	Click to copy an existing fax protocol to a new fax protocol. In the box that appears, select an existing fax protocol, enter new name if desired, and click **Copy**.	–
Name	Name of the fax protocol. This name is used when you copy an existing fax profile to a new fax profile.	–

Primary	Select from a set of fax protocol options. Each option is a bundled set of related fax commands.
	For a detailed description of each bundle, see the "Primary Fax Protocol Command Bundles" table
	The descriptions of the bundles include the following components:
	• **nse**–Uses NSEs to switch to T.38 fax relay mode
	• **force**–Unconditionally uses Cisco Network Services Engines (NSE) to switch to T.38 fax relay
	• **version**–Specifies a version for configuring fax speed:
	  • **0**–Configures version 0, which uses T.38 version 0 (1998-G3 faxing)
	  • **3**–Configures version 3, which uses T.38 version 3 (2004-V.34 or SG3 faxing)
	• **none**–No fax pass-through or T.38 fax relay is attempted
	• **Pass-through**–The fax stream uses one of the following high-bandwidth codecs:
	  • **g711ulaw**–Uses the G.711 ulaw codec
	  • **g711alaw**–Uses the G.711 alaw codec
		fax protocol { **none** | **pass-through** {**g711ulaw** | **g711alaw**} [**fallback none**]| **t38** [**nse** [**force**]] [**version** {**0** | **3**}] [**ls-redundancy** *value* [**hs-redundancy** *value*]] [**fallback** {**none** | **pass-through** {**g711ulaw** | **g711alaw**}}]}

Fallback	Available when the primary protocol bundle name that you selected in the Primary field begins with "T.38" or with "Fax Pass-through." Select the fallback mode for fax transmissions. This fallback mode is used if the primary fax protocol cannot be negotiated between device endpoints. For a detailed description of each option, see the "Fallback Protocol Options" table.	**fax protocol** {none | pass-through {g711ulaw | g711alaw} [**fallback none**] | t38 [nse [force]] [version {0 | 3}] [ls-redundancy value [hs-redundancy value]] [**fallback** {**none** | **pass-through** {**g711ulaw** | **g711alaw**}}]}

Option	Description	Cisco IOS CLI Equivalent
Low Speed	Available when the primary protocol bundle name that you selected in the Primary field begins with "T.38." Specifies the number of redundant T.38 fax packets to be sent for the low-speed V.21-based T.30 fax machine protocol. Range: varies from 0 (no redundancy) to 5. Default: 0.	**ls-redundancy** *value*
High Speed	Available when the primary protocol bundle name that you selected in the Primary field begins with "T.38." Specifies the number of redundant T.38 fax packets to be sent for high-speed V.17, V.27, and V.29 T.4 or T.6 fax machine image data. Range: varies from 0 (no redundancy) to 2. Default: 0	**hs-redundancy** *value*
Save Fax Protocol	Click to save the configuration settings that you made.	–

The following table describes the bundled sets of fax commands that are available for the Primary option when you configure the fax protocol capability for a SIP dial peer endpoint.

For low speed (ls) redundancy, the range varies from 0 (no redundancy) to 5. For high speed (HS redundancy, the range varies from 0 (no redundancy) to 2.

Table 47: Primary fax protocol command bundles

Fax Command Protocol Bundle	Description	Cisco IOS CLI Equivalent
T.38 Fax Relay Version 3	Primary fax protocol is T.38 fax relay version 3. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 3 ls-redundancy** *value* **hs-redundancy** *value* **no fax-relay sg3-to-g3**
T.38 Fax Relay Version 0	Primary fax protocol is T.38 fax relay version 0. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 ls-redundancy** *value* **hs-redundancy** *value*
T.38 Fax Relay Version 3 NSE	Primary fax protocol is NSE based T.38 fax relay version 3. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 3 nse ls-redundancy** *value* **hs-redundancy** *value* **no fax-relay sg3-to-g3**

Fax Command Protocol Bundle	Description	Cisco IOS CLI Equivalent
T.38 Fax Relay Version 3 NSE force	Primary fax protocol is NSE force option of T.38 fax relay version 3. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 3 nse force ls-redundancy** *value* **hs-redundancy** *value* **no fax-relay sg3-to-g3**
T.38 Fax Relay Version 0 NSE	Primary fax protocol is NSE option of T.38 fax relay version 0. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 nse ls-redundancy** *value* **hs-redundancy** *value*
T.38 Fax Relay Version 0 NSE force	Primary fax protocol is NSE force option of T.38 fax relay version 0. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 nse force ls-redundancy** *value* **hs-redundancy** *value*
T.38 Fax Relay Version 0 No ECM	Primary fax protocol is T.38 fax relay version 0 with ECM disabled. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 ls-redundancy** *value* **hs-redundancy** *value* **fax-relay ecm disable**
T.38 Fax Relay Version 0 NSE No ECM	Primary fax protocol is NSE based T.38 fax relay version 0 with ECM disabled. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 nse ls-redundancy** *value* **hs-redundancy** *value* **fax-relay ecm disable**
T.38 Fax Relay Version 0 NSE force No ECM	Primary fax protocol is NSE force option T.38 fax relay version 0 with ECM disabled. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 nse force ls-redundancy** *value* **hs-redundancy** *value* **fax-relay ecm disable**
T.38 Fax Relay Version 0 Rate 14.4 No ECM	Primary fax protocol is T.38 fax relay version 0 with ECM disabled and fax rate of 14,400 bps. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 ls-redundancy** *value* **hs-redundancy** *value* **fax-relay ecm disable** **fax rate 14400**
T.38 Fax Relay Version 0 NSE Rate 14.4 No ECM	Primary fax protocol is NSE based T.38 fax relay version 0 with ECM disabled and fax rate of 14,400 bps. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 nse ls-redundancy** *value* **hs-redundancy** *value* **fax-relay ecm disable** **fax rate 14400**

Fax Command Protocol Bundle	Description	Cisco IOS CLI Equivalent
T.38 Fax Relay Version 0 NSE force Rate 14.4 No ECM	Primary fax protocol is NSE force option T.38 fax relay version 0 with ECM disabled and fax rate of 14,400 bps. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 nse force ls-redundancy** *value* **hs-redundancy** *value* **fax-relay ecm disable** **fax rate 14400**
T.38 Fax Relay Version 0 Rate 9.6 No ECM	Primary fax protocol is T.38 fax relay version 0 with ECM disabled and fax rate of 9,600 bps Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 ls-redundancy** *value* **hs-redundancy** *value* **fax-relay ecm disable** **fax rate 9600**
T.38 Fax Relay Version 0 NSE Rate 9.6 No ECM	Primary fax protocol is NSE based T.38 fax relay version 0 with ECM disabled and fax rate of 9,600 bps. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 nse ls-redundancy** *value* **hs-redundancy** *value* **fax-relay ecm disable** **fax rate 9600**
T.38 Fax Relay Version 0 NSE force Rate 9.6 No ECM	Primary fax protocol is NSE force option T.38 fax relay version 0 with ECM disabled and fax rate of 9,600 bps. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 nse force ls-redundancy** *value* **hs-redundancy** *value* **fax-relay ecm disable** **fax rate 9600**
T.38 Fax Relay Version 0 Rate 14.4	Primary fax protocol is T.38 fax relay version 0 with ECM and fax rate of 14,400 bps. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 ls-redundancy** *value* **hs-redundancy** *value* **fax rate 14400**
T.38 Fax Relay Version 0 NSE Rate 14.4	Primary fax protocol is NSE based T.38 fax relay version 0 with ECM and fax rate of 14,400 bps. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 nse ls-redundancy** *value* **hs-redundancy** *value* **fax rate 14400**
T.38 Fax Relay Version 0 NSE force Rate 14.4	Primary fax protocol is NSE force option T.38 fax relay version 0 with ECM and fax rate of 14,400 bps. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 nse force ls-redundancy** *value* **hs-redundancy** *value* **fax rate 14400**

Fax Command Protocol Bundle	Description	Cisco IOS CLI Equivalent
T.38 Fax Relay Version 0 Rate 9.6	Primary fax protocol is T.38 fax relay version 0 with ECM and fax rate of 9,600 bps. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 ls-redundancy** *value* **hs-redundancy** *value* **fax rate 9600**
T.38 Fax Relay Version 0 NSE Rate 9.6	Primary fax protocol is NSE based T.38 fax relay version 0 with ECM and fax rate of 9,600 bps. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 nse ls-redundancy** *value* **hs-redundancy** *value* **fax rate 9600**
T.38 Fax Relay Version 0 NSE force Rate 9.6	Primary fax protocol is NSE force option T.38 fax relay version 0 with ECM and fax rate of 9,600 bps. Options for selecting the low-speed and high-speed redundancy values are available.	**fax protocol t38 version 0 nse force ls-redundancy** *value* **hs-redundancy** *value* **fax rate 9600**
None	Fax protocol is disabled.	**fax protocol none**
Fax Pass-through G711ulaw	Primary fax protocol is fax pass-through with pass-through codec set to g711ulaw.	**fax protocol pass-through g711ulaw**
Fax Pass-through G711ulaw No ECM	Primary fax protocol is fax pass-through with pass-through codec set to g711ulaw and ECM disabled.	**fax protocol pass-through g711ulaw** **fax-relay ecm disable**
Fax Pass-through G711alaw	Primary fax protocol is fax pass-through with pass-through codec set to g711alaw.	**fax protocol pass-through g711alaw**
Fax Pass-through G711alaw No ECM	Primary fax protocol is fax pass-through with pass-through codec set to g711alaw and ECM disabled.	**fax protocol pass-through g711alaw** **fax-relay ecm disable**

The following table describes the selections that are available for the Fallback option when you configure the fax protocol capability for a SIP dial peer endpoint.

Table 48: Fallback protocol options

Fallback Fax Protocol Options	Description	Cisco IOS CLI Equivalent
None	Fallback Fax Protocol is None. All special fax handling is disabled.	**fax protocol t38** [**nse** [**force**]] [**version** {**0** | **3**}] [**ls-redundancy** *value* [**hs-redundancy** *value*]] **fallback none** **fax protocol pass-through** {**g711ulaw** | **g711alaw** } **fallback none**

Fallback Fax Protocol Options	Description	Cisco IOS CLI Equivalent
Fax Pass-through G711ulaw	Fallback Fax Protocol is Fax Pass-through with pass-through codec set to g711ulaw.	**fax protocol t38** [**nse** [**force**]] [**version** {**0** | **3**}] [**ls-redundancy** *value* [**hs-redundancy** *value*]] **fallback pass-through g711ulaw**
Fax Pass-through G711alaw	Fallback Fax Protocol is Fax Pass-through with pass-through codec set to g711alaw.	**fax protocol t38** [**nse** [**force**]] [**version** {**0** | **3**}] [**ls-redundancy** *value* [**hs-redundancy** *value*]] **fallback pass-through g711alaw**

Configure SRST phones for a voice policy

Configure SRST phones for a voice policy

This task defines how the system augments and manipulates calls for the Cisco Unified SRST phone endpoint type within a voice policy. It allows you to configure media profile options for phones operating in SRST mode.

When configuring SRST phones for a voice policy, you define the codecs and DTMF relay options that will be available for phones registered to the local gateway when in Cisco Unified SRST mode. These settings ensure proper call functionality during WAN outages or degradation.

Before you begin

You must be in the process of adding a new voice policy or editing an existing one within Cisco SD-WAN Manager

Follow these steps to configure SRST phones for a voice policy:

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Unified Communications**
2. Click **Add Voice Policy**, and choose **SRST Phone**.
3. From the **Add SRST Phone Policy Profile** drop-down list, select **Create New**.

   Alternatively, you can select **Copy from Existing** to reuse settings from an existing policy profile.
4. Configure the Media Profile:
   a) Click **Media Profile**, and click **Next**.
   b) Click **Add New Media Profile**.
   c) In the page that displays, configure options as described in the Voice policy SRST phones configuration options on page 118 topic.

      Define the codecs and DTMF relay options for SRST phones.
5. Click **Next**.
6. In **Policy Profile Name**, enter a name for this child policy.
7. In **Policy Profile Description**, enter a description for this child policy.
8. Click **Save**.

The SRST phones for the voice policy are successfully configured.

What to do next

You have now configured all subpolicies for the Add a Voice Policy supertask. Proceed to provision a device template for Unified Communications to apply this voice policy to your devices.

Voice policy SRST phones configuration options

Voice policy SRST phones configuration options

This reference topic describes the options available for configuring SRST (Survivable Remote Site Telephony) phones within a voice policy. These settings define the media profile, including codecs and DTMF relay options, for phones operating in Cisco Unified SRST mode.

Table 49: Voice policy SRST phones configuration options

Option	Description	Cisco IOS CLI Equivalent
Medial Profile Number	Enter a number for this Cisco Unified SRST media profile. Valid range: Integers 1 through 10000.	**voice class codec** *tag-number*
Codec	Move from the Source list to the Target list the codecs that you want to be available for phones when they are in Cisco Unified SRST mode and communicating with other phones that are in the same site and registered to the same gateway. Codecs in the target list are in descending order of priority, with the highest priority at the top of the list. Drag and drop items in this list to rearrange them.	**voice class codec** *tag-number* **codec preference** *value codec-type*
DTMF field	Move from the source list to the target list the DTMF relay options that you want the system to use when in Cisco Unified SRST mode. Items in the target list are in descending order of priority, with the highest priority at the top of the list. Drag and drop items in this list to rearrange them. If you want to include the **Inband** option in the Target list, it can be the only option in that list. If you want to include other options in the Target list, move the Inband option to the Source list before saving the media profile.	**dtmf-relay** {[[**sip-notify**] [**sip-kpml**] [**rtp-nte**]]}
Save	Click to save the configuration settings that you made.	–

Provision a device template for unified communications

Provision a device template for unified communications

This task allows you to select UC-specific feature templates and set up the voice policy to include with a device template. This process applies the configured Unified Communications settings to your devices.

A device template bundles various feature templates and policies, enabling consistent and scalable deployment of configurations across multiple devices. This task is the final step in preparing your UC voice services for deployment.

Before you begin

Ensure that all necessary UC-specific feature templates (Voice Card, Call Routing, SRST, DSPFarm) and voice policies have been previously created and configured.

Follow these steps to provision a device template for Unified Communications:

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**, and click **Create Template**.

   > **Note**
   >
   > In Cisco vManage Release 20.7.1 and earlier releases, **Device Templates** is called **Device**.

3. From the **Create Template** drop-down list, select **From Feature Template**.
4. From the **Device Model** drop-down list, select the type of supported device to which you want to attach the UC-specific feature templates and map the voice policy.
5. Click **Unified Communications**.
6. To select UC-specific feature templates to include with the device template, perform these actions:
   a) From the **Voice Card** drop-down list, select the voice card feature template.
   b) From the Call Routing drop-down list, select the call routing feature template.
   c) From the SRST drop-down list, select the SRST feature template.
   d) From the DSPFarm drop-down list, select the DSPFarm template.
7. To set up the voice policy to include with the device template, perform these actions:
   a) From the **Voice Policy** drop-down list, select the voice policy.
   b) Click **Mapping**.
   c) From the list of endpoint types in the left pane of the screen that displays, select the type of endpoint that contains the subpolicies that you want to map to specific endpoints.
   d) From the list of subpolicies that displays, click **...**, and select **Mapping** for the subpolicy that you want to map to specific endpoints.
   e) In the list of endpoints that displays, select each endpoint to which you want to map the subpolicy
   f) Click **Map**.
   g) Click **Save**.

   When you map subpolicies to endpoints, the system generates the CLI commands. See Generated CLI commands for subpolicies to endpoints mapping on page 120.
8. To create the device template, click **Create**.

A device template for Unified Communications is successfully provisioned, including the selected UC-specific feature templates and voice policy mappings.

What to do next

The device template is now ready to be attached to devices to deploy the Unified Communications configurations.

Generated CLI commands for subpolicies to endpoints mapping

Details the automatically generated CLI commands used when mapping subpolicies—such as translation profiles, media profiles, supervisory disconnect, trunk group, modem pass-through, and fax protocol—to various endpoints in a device template, providing insight into their configuration and application.

This reference topic describes the CLI commands that are automatically generated when subpolicies are mapped to specific endpoints within a device template. This table provides insight into the underlying configuration applied by the Cisco SD-WAN Manager.

Table 50: Generated CLI commands for subpolicies to endpoints mapping

Endpoint	Subpolicy	Cisco IOS CLI Application Mapping	Remarks
Voice Port FXO Voice Port FXS Voice Port FXS DID Voice Port PRI ISDN POTS Dial Peer SIP Dial Peer	Translation profile	**translation-profile incoming** *profile-name* **translation-profile outgoing** *profile-name*	A translation profile policy is applied to a dial peer or a voice profile.
SRST Phone SIP Dial Peer	Media profile	voice register pool *number* **voice-class codec** *number* **dtmf-relay** {[[**sip-notify**] [**sip-kpml**] [**rtp-nte**]]}	A media profile policy includes voice class codec and DTMF relay configurations. This policy is applied to an incoming SIP dial peer, an outgoing SIP dial peer, or an SRST phone profile.
Voice Port FXO	Supervisory disconnect	voice port *number* **supervisory custom-cptone** *cptone-name* **supervisory dualtone-detect=params** *tag*	A supervisory disconnect policiy such as custom-cptone or dualtone-detect-params is applied to FXO voice interfaces.
Voice Port FXO Voice Port FXS Voice Port FXS DID Voice Port PRI ISDN POTS Dial Peer	Trunk group	**trunk-group name** [*preference-num*] **voice-port** *number* *trunk-group name* [*preference-num*] **interface serial** *slot*/*sub-slot*/**port:{15 | 23}** **dial-peer voice** *tag* **pots** **trunkgroup name** *preference-num*	If more than one interface is assigned to the same trunk group, the *preference-num* value determines the order in which the trunk group uses the interfaces. A preference-num value of 1 is the highest preference, so an interface with that value is used first. A value of 64 is the lowest preference so an interface with that value is used last.

Endpoint	Subpolicy	Cisco IOS CLI Application Mapping	Remarks
SIP Dial Peer	Modem pass-through	None: **no modem passthrough** G.711 ulaw: **modem passthrough nse codec g711ulaw** G.711 alaw: **modem passthrough nse codec g711alaw**	–
SIP Dial Peer	Fax protocol	**fax protocol** {**none** | **pass-through** {**g711ulaw** | **g711alaw**} [**fallback none**] | **t38** [**nse** [**force**]] [**version** {**0** | **3**}] [**ls-redundancy** *value* [**hs-redundancy** *value*]] [**fallback** {**none** | **pass-through** {**g711ulaw** | **g711alaw**}}]}	–

Dial peer CSV file

Dial peer CSV file

This reference topic describes the structure and content requirements for a Dial Peer CSV (Comma Separated Values) file. This file includes information for one or more incoming and outgoing SIP and POTS dial peers, allowing for bulk configuration or import into Cisco SD-WAN Manager.

The file must be comma delimited, and each record in the file must include each field that the following table describes, in the order shown.

Table 51: Dial peer CSV file

Field	Description
Dial Peer Tag	Number that is used to reference the dial peer.
Dial Peer Type	Type of dial peer that you are creating (**pots** or **voip**).
Direction	Direction of traffic on the dial peer (**Incoming** or **Outgoing**).
Description	Description of the dial peer.

Field	Description
Forward Digits	How the dial peer transmits digits in outgoing numbers: • **All**–The dial peer transmits all digits in the number. • **None**–The dial peer does not transmit digits in the number that do not match the destination pattern. • *n*–The dial peer transmits the number of right-most digits in the number that the integer *n* represents. For example, if *n* is 7 and the outgoing number is 1112223333, the dial peer transmits 2223333.
Preference	For POTS dial peers, a unique numeric value for the dial peer. If dial peers have the same match criteria, the system uses the one with the highest preference value.
Prefix	Digits to be prepended to outgoing POTS dial peer calls.
Numbering Pattern	String that the router uses to match incoming calls to the dial peer.
Dest. Address	Network address of the remote voice gateway to which calls are sent after a local outgoing SIP dial peer is matched.
Voice Port	Voice port that the router uses to match calls to the dial peer. For an outgoing dial peer, the router sends the calls that match the dial peer to this port. For an incoming dial peer, this port serves as an additional match criterion. The dial peer is matched only if a call comes in on this port.
Transport Protocol	For SIP dial peers, transport protocol (**TCP** or **UDP**) for SIP control signaling.

Example dial peer CSV file

```
Tag,type,Direction,Description,Forward Digits,Preference,Prefix,Pattern,Dest.
 Address,Voice Port,Transport
6545,voip,Outgoing,description To Voice Gateway,,1,,23456,ipv4:166.2.121.17,,udp
6756,voip,Outgoing,description ***Fax Number
6362-6362***,,0,,34567,ipv4:166.2.121.16,,tcp
768,voip,Outgoing, description Fire Alarm Dialer,,8,,5678,ipv4:166.2.121.19,,udp
10,pots,Incoming,,,5,,0115T,,1/0/1,
54,pots,Outgoing,,,6,,.T,,1/0/3,
23,pots,Incoming,,all,0,,76..,,1/0/4,
26,pots,Incoming,,5,1,55,9800........,,1/0/5,
27,pots,Incoming,,5,1,55,9800........,,0/1/5:15,
```

Translation rules CSV file

Translation rules CSV file

This reference topic describes the structure and content requirements for a Translation Rules CSV (Comma Separated Values) file. This file can be used to import existing translation rule information when configuring translation profiles for voice policies.

The file must be comma delimited, and each record in the file must include each field that the following table describes, in the order shown.

Table 52: Translation rules CSV file

Field	Description
Match	String that you want the translation rule to affect. The string must be in regular expression format beginning and ending with a slash (/). For example, /^9/.
Action	Action that the system performs for calls that match the string in the Match field. Valid values are: • **reject**–Causes the system to reject the call • **replace**–Causes the system to replace the match string with the value in the Replace field
Replace	If the Action field contains **replace**, this field contains the string to which to translate the matched string. Enter the number in regular expression format beginning and ending with a slash (/). For example, //, which indicates a replacement of no string. As an example, if you specify a match string of /^9/ and a replace string of //, the system removes the leading 9 from calls with a number that begins with 9. In this case, the system translates 914085551212 to 14085551212.

Example translation rules CSV file

This section provides an example of a Translation Rules CSV file, illustrating the format and content described above.

```
Match,Action,Replace
/34/,replace,/34/
/23/,reject,
/56/,replace,/100/
/16083652563/,replace,/6083652563/
```

Monitor UC operations

Monitor UC operations

This task allows you to monitor the real-time statuses of lines, calls, interfaces, and related items that a device processes after enabling UC voice services for supported routers.

Monitoring UC operations provides crucial insights into the performance and status of your Unified Communications deployment, helping you verify functionality and troubleshoot issues.

Before you begin

UC voice services must be enabled for the supported routers you wish to monitor.

Follow these steps to monitor UC operations:

Procedure

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

   Note

   Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. In the table of devices, select the device for which you want to monitor UC operations.
3. From **Security Monitoring**, click **Real Time**.
4. In **Device Options**, select one of these options:
   a) **Voice Calls**: Displays information for active voice calls. See Voice calls monitoring information on page 124 table.
   b) **Voice VOIP Calls**: Displays information for active VOIP calls. See Voice VoIP calls monitoring information on page 125 table.
   c) **Voice Phone Info**: Displays information about Cisco Unified SRST registrations. See Voice phone info monitoring information on page 125 table.
   d) **Voice Controller T1 E1 Current 15 mins Stats**: Displays configuration and status information for the T1/E1 voice module that is installed in the device, compiled over the past 15 minutes. See Voice controller T1 E1 current 15 Mins stats monitoring information on page 126 table.
   e) **Voice Controller T1 E1 Total Stats**: Displays configuration and status information for the T1/E1 voice module that is installed in the device, compiled since the module last started. See Voice controller T1 E1 total stats monitoring information on page 127 table.
   f) **Voice ISDN Status**: Displays information about Layer 1 and Layer 2 status for the ISDN controller, and information about active calls. See Voice ISDN status information on page 128 table.
   g) **Voice DSPFarm SCCP CUCM Groups**: Displays detailed information about Cisco Unified Communications Manager groups that are configured for DSP farm services on a device. See Voice DSPFarm SCCP CUCM groups monitoring information on page 128 table.
   h) **Voice DSPFarm Profile**: Displays detailed information about DSP farm service profiles and media resources that are configured on the device. See Voice DSPFarm profile monitoring information on page 129 table.
   i) **Voice DSP Farm SCCP Connections**: Displays detailed information about SCCP connections between the device and Cisco Unified Communications Manager. See Voice DSPFarm SCCP connections monitoring information on page 130 table.
   j) **Voice DSPFarm Active**: Displays operational and status information about DSP farm resources that are active on the device. See Voice DSPFarm active monitoring information on page 131 table.
   k) **Interface Detail**: Displays status and statistical information for interfaces that are configured for the router.
   l) **Interface Statistics**: Displays statistical information for interfaces that are configured for the router
   m) **Interface T1/E1**: Displays information for the T1/E1 voice module that is installed in the device

Real-time operational data for the selected UC services is displayed, providing insight into their status and performance.

Voice calls monitoring information

Describes the information available when monitoring active voice calls, including call ID, voice port, codec, VAD, DSP details, and packet statistics such as transmitted, received, and aborted packets, as well as the last update time.

This reference topic describes the information displayed when monitoring active voice calls on a device. It provides details such as call ID, voice port, codec used, and packet statistics.

Table 53: Voice calls monitoring information

Field	Description
Call ID	System assigned identifier of a telephony call leg
Voice Port	Voice port used for the call
Codec	Negotiated codec used for the call
VAD	Indicates whether VAD is enabled or disabled for the call
DSP Cannel	DSP channel used for the call
DSP Type	Type of DSP used for the call
Aborted Packets	Number of packets aborted during the call
TX Packets	Number of packets transmitted during the call
RX Packets	Number of packets received during the call
Last Updated	Date and time when the information on this page was last updated

Voice VoIP calls monitoring information

Details the information available when monitoring active VoIP calls, including call ID, codec, destination address and port, RTP packet statistics, call duration, and the timestamp of the last update.

This reference topic describes the information displayed when monitoring active VoIP calls on a device. It provides details such as call ID, codec, destination address, and packet statistics for RTP connections.

Table 54: Voice VoIP calls monitoring information

Field	Description
Call ID	System assigned identifier of an RTP connection for a call leg
Codec	Negotiated codec used for the call
Destination Address	IP address of the destination of the call
Destination Port	RTP port of the destination of the call
TX Packets	Number of packets transmitted during the call
RX Packets	Number of packets received during the call
Duration (ms)	Duration of the call, in milliseconds
Last Updated	Date and time when the information on this page was last updated

Voice phone info monitoring information

Details the fields displayed when monitoring voice phone information for Cisco Unified SRST registrations, including phone pool tags, network identifiers, registration states, dialpeer tags, device addresses, directory numbers, and update timestamps.

This reference topic describes the information displayed when monitoring voice phone information, specifically related to Cisco Unified SRST registrations on a device. It includes details about phone pools, network identifiers, and registration states.

Table 55: Voice phone info monitoring information

Field	Description
Pool Tag	Tag number that is assigned to the Cisco Unified SRST phone pool on the device
ID Network	Identifier of the network subnet that the device uses to register phones that fallback from Cisco Unified Communications Manager to this device
Registration State	Indicates whether phones that are in Cisco Unified SRST mode are registered to this device
Dialpeer Tag	System assigned tag used by the dial peer that is assigned to the directory number of phones that are in Cisco Unified SRST mode and are registered to this device
Address	IP address of the device interface that is used for SIP SRST call control when phones fail over
Directory Number	Directory number of each phone that is in Cisco Unified SRST mode
Last Updated	Date and time when the information on this page was last updated

Voice controller T1 E1 current 15 Mins stats monitoring information

Voice controller T1 E1 current 15 Mins stats monitoring information

This reference topic describes the configuration and status information displayed for a T1/E1 voice module, compiled over the past 15 minutes. It includes details such as interface status, clock source, and various error statistics.

Table 56: Voice controller T1 E1 current 15 Mins stats monitoring information

Field	Description
Interface-slot-num	Slot number of the controller.
Insterface-subslot-num	Subslot number of the controller.
Interface-port-num	Port number of the controller.
Status	Status of the controller.
Type	Type of the controller.
Clock Source	Clock source used for the controller.
Line Code Violations	Number line code violations that have occurred.
Path Code Violations	Number path code violations that have occurred.
Slip Seconds	Number of slip seconds that have occurred. A slip can occur when there is a difference between the timing of a synchronous receiving terminal and the received signal.

Field	Description
Frame Loss Seconds	Number of seconds in which out of frame (OOF) errors have occurred.
Line Err. seconds	Number of seconds in which Line Errored Seconds (LES) have occurred. A LES is a second in which one or more Line Code Violation errors are detected.
Degraded Minutes	Number of Degraded Minutes that have occurred. A Degraded Minute is one in which the estimated error rate exceeds 1E-6 but does not exceed 1E-3.
Errored Seconds	Number of Errored Seconds that have occurred.
Bursty Errored Seconds	Number of Bursty Error Seconds that have occurred. A Bursty Error Second is a second with less than 320 and more than 1 path coding violation errors, no severely errored frame defects, and no detected incoming AIS defects.
Severely Errored Seconds	Number of Severely Errored Seconds that have occurred.
Unavailable Seconds	Number of Unavailable Seconds that have occurred. This value is calculated by counting the number of seconds that the interface is unavailable.
Last Updated	Date and time when the information on this page was last updated.

Voice controller T1 E1 total stats monitoring information

Voice controller T1 E1 total stats monitoring information

This reference topic describes the configuration and status information displayed for a T1/E1 voice module, compiled since the device last started. It includes cumulative details such as interface status, clock source, and various error statistics.

Table 57: Voice controller T1 E1 total stats monitoring information

Field	Description
Interface-slot-num	Slot number of the controller.
Insterface-subslot-num	Subslot number of the controller.
Interface-port-num	Port number of the controller.
Status	Status of the controller.
Type	Type of the controller.
Clock Source	Clock source used for the controller.
Line Code Violations	Number line code violations that have occurred.
Path Code Violations	Number path code violations that have occurred.
Slip Seconds	Number of slip seconds that have occurred. A slip can occur when there is a difference between the timing of a synchronous receiving terminal and the received signal.
Frame Loss Seconds	Number of seconds in which out of frame (OOF) errors have occurred

Field	Description
Line Err. seconds	Number of seconds in which Line Errored Seconds (LES) have occurred. A LES is a second in which one or more Line Code Violation errors are detected.
Degraded Minutes	Number of Degraded Minutes that have occurred. A Degraded Minute is one in which the estimated error rate exceeds 1E-6 but does not exceed 1E-3.
Errored Seconds	Number of Errored Seconds that have occurred.
Bursty Errored Seconds	Number of Bursty Error Seconds that have occurred. A Bursty Error Second is a second with less than 320 and more than 1 path coding violation errors, no severely errored frame defects, and no detected incoming AIS defects.
Severely Errored Seconds	Number of Severely Errored Seconds that have occurred.
Unavailable Seconds	Number of Unavailable Seconds that have occurred. This value is calculated by counting the number of seconds that the interface is unavailable.
Last Updated	Date and time when the information on this page was last updated.

Voice ISDN status information

Voice ISDN status information

This reference topic describes the information displayed when monitoring voice ISDN status on a device. It provides details about Layer 1 and Layer 2 status for the ISDN controller and information about active calls.

Table 58: Voice ISDN status information

Field	Description
Key ID	Identifier of the table row
Interface	Name of the PRI ISDN digital interface
Switch Type	Switch type used for the PRI ISDN digital interface
Layer 1 Status	Layer 1 status of the PRI ISDN digital interface
Layer 2 Status	Layer 2 status of the PRI ISDN digital interface
Active Calls	Number of active calls on the PRI ISDN digital interface
Last Updated	Date and time when the information on this page was last updated

Voice DSPFarm SCCP CUCM groups monitoring information

Voice DSPFarm SCCP CUCM groups monitoring information

This reference topic describes the detailed information displayed when monitoring Cisco Unified Communications Manager groups configured for DSP farm services on a device. It includes group IDs, switchover/switchback methods, and associated profiles.

Table 59: Voice DSPFarm SCCP CUCM groups monitoring information

Field	Description
CUCM Group ID	Identifier of the Cisco Unified Communications Manager group
Description	Description of the Cisco Unified Communications Manager group
Switchover Method	Method that the primary Cisco Unified Communications Manager server in this Cisco Unified Communications Manager group uses for failover
Switchback Method	Method that the secondary Cisco Unified Communications Manager server in this Cisco Unified Communications Manager group uses to switch back after a failover
CUCM ID	Identifier of each Cisco Unified Communications Manager server in the Cisco Unified Communications Manager group
CUCM Priority	Priority in which the Cisco Unified Communications Manager servers in this Cisco Unified Communications Manager group are used
Profile ID	Identifier of the DSP farm profile that is registered to each Cisco Unified Communications Manager server in the Cisco Unified Communications Manager group
Reg. Name	Name of the DSP farm profile that is registered to each Cisco Unified Communications Manager server in the Cisco Unified Communications Manager group
Last Updated	Date and time when the information on this page was last updated

Voice DSPFarm profile monitoring information

Voice DSPFarm profile monitoring information

This reference topic describes the detailed information displayed when monitoring DSP farm service profiles and media resources configured on a device. It includes profile IDs, service types, operational status, and resource information.

Table 60: Voice DSPFarm profile monitoring information

Field	Description
Profile ID	Identifier of the DSP farm profile.
Service ID	Type of DSP farm service that is configured for this DSP farm profile.
Service Mode	Service mode for this DSP farm profile.
Resource ID	Resource identifier for the DSP resource group in this DSP farm profile.
Admin	Status of this DSP farm profile. If this field displays DOWN, ensure that the Shutdown option is not enabled in the Profile tab of the DSPFarm feature template that defines this DSP farm.

Field	Description
Operation	Status of the registration of the profile with Cisco Unified Communications Manager: • ACTIVE IN PROGRESS–Profile is in the process of registering with Cisco Unified Communications Manager • DOWN–Profile is unable to register with Cisco Unified Communications Manager • ACTIVE– Profile is registered with Cisco Unified Communications Manager
App. Type	Type of application with which the DSP farm services that are provisioned on the device are associated.
App. Status	Status of the association of this profile with Cisco Unified Communications Manager: • app-assoc-done–Profile is associated with Cisco Unified Communications Manager • app-assoc-not-done–Profile is not associated with Cisco Unified Communications Manager
Resource Provider	Information about the mediaresource family that relates to the profile.
Provider Status	Status of the media resources that relate to the profile.
Last Updated	Date and time when the information on this page was last updated.

Voice DSPFarm SCCP connections monitoring information

Voice DSPFarm SCCP connections monitoring information

This reference topic describes the detailed information displayed when monitoring SCCP connections between a device and Cisco Unified Communications Manager. It includes connection IDs, session types, codecs, and remote/local endpoint details.

Table 61: Voice DSPFarm SCCP connections monitoring information

Field	Description
Connection ID	Identifier of an SCCP connection for an active call that uses this DSP farm service
Session ID	Identifier of an SCCP session for an active call that uses this DSP farm service
Session Type	Type of DSP farm service for this SCCP connection
Mode	Mode for direction of traffic for this SCCP connection
Codec	Codec provisioned for this SCCP connection
Remote IP	IP address of the remote endpoint for this SCCP connection
Remote Port	Port number of the remote endpoint for this SCCP connection

Field	Description
Source Port	Port number of the local endpoint for this SCCP connection
Last Updated	Date and time when the information on this page was last updated

Voice DSPFarm active monitoring information

Voice DSPFarm active monitoring information

This reference topic describes the operational and status information displayed for active DSP farm resources on a device. It includes details about DSP identifiers, status, and packet counts for active connections.

Table 62: Voice DSPFarm active monitoring information

Field	Description
DSP	Identifier of the DSP for an active call that uses this DSP farm service
Status	Status of the DSP for an active call that uses this DSP farm service
Resource ID	Resource Identifier that is associated with the DSP that this connection uses
Bridge ID	Bridge Identifier that is associated with the DSP that this connection uses
Transmit Packets	Number of packets that this connection has transmitted
Received Packets	Number of packets that this connection has received
Last Updated	Date and time when the information on this page was last updated

5 Cisco Unified Communications FXS and FXO Caller ID

Topics:

- Feature History for Cisco Unified Communications FXS and FXO Caller ID
- Cisco Unified Communications FXS and FXO Caller ID Support
- Supported devices for adding voice features with CLI add-on feature templates
- Restrictions for Adding Voice Features with a CLI Add-On Feature Template
- Voice-feature configuration commands for a CLI add-on Feature Template

Introduces FXS and FXO Caller ID features within Cisco Unified Communications, outlining their functions and integration for enhanced telephony capabilities.

Feature History for Cisco Unified Communications FXS and FXO Caller ID

Outlines the feature history and release information for Cisco Unified Communications FXS and FXO Caller ID, including support for configuring caller ID features using Cisco SD-WAN Manager CLI add-on templates.

Table 63: Feature History

Feature Name	Release Information	Description
Cisco Unified Communications FXS and FXO Caller ID Support	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco Catalyst SD-WAN Manager Release 20.18.1	This feature lets you configure Foreign Exchange Station (FXS) and Foreign Exchange Office (FXO) caller ID features by using Cisco SD-WAN Manager CLI add-on feature templates.

Cisco Unified Communications FXS and FXO Caller ID Support

Outlines FXS and FXO caller ID configuration and management, including per-port settings, CLI add-on template usage, signaling type changes, and guidance to prevent configuration mismatches between device and network setups.

Caller ID is an analog service that

- enables a telephone central office switch to send digital information about an incoming call,
- is configurable on a per-port basis for analog FXS ports and is also available on analog FXO ports, and
- relies on the identity of the calling party for its features and requires proper configuration management to prevent mismatches between device and network configurations.

You can configure FXS and FXO caller ID features in Cisco IOS XE Catalyst SD-WAN device by using CLI add-on feature templates. For detailed information about CLI add-on feature templates, see CLI Add-On-Feature Templates.

If an FXS voice port has caller ID commands configured, remove all the caller-id configurations before changing the signaling type from loop-start or ground-start to Direct Inward Dialing (DID).

If you remove a voice port from a device after a caller ID command is configured, remove the caller ID configuration from the device. Otherwise, a voice port configuration mismatch occurs between the Cisco IOS configuration and the Cisco Catalyst SD-WAN configuration.

Supported devices for adding voice features with CLI add-on feature templates

Lists Cisco network interface and service modules that support voice features when configured with CLI add-on feature templates.ß

This section provides Cisco network interface and service modules that are compatible with voice features using CLI-add-on templates.

- Cisco NIM-2FXO network interface module
- Cisco NIM-4FXO network interface module
- Cisco NIM-2FXSP network interface module
- Cisco NIM-4FXSP network interface module
- Cisco NIM-2FXS/4FXOP network interface module

- Cisco SM-X-72FXS double-wide service module
- Cisco SM-X-24FXS/4FXO single-wide service module
- Cisco SM-X-16FXS/2FXO single-wide service module
- Cisco SM-X-8FXS/12FXO single-wide service module

Restrictions for Adding Voice Features with a CLI Add-On Feature Template

Outlines key restrictions for adding voice features with a CLI add-on feature template, including prerequisite caller ID enablement and considerations for network stability when managing DSP resources on FXO voice ports.ß

Enable Caller ID Before Configuring Caller ID

Caller ID must be enabled with the command before you use any other caller ID–related commands.

Network Stability When Allocating or Deallocating DSP Resources

When using or disabling the **caller-id alerting dsp-pre-allocate** command, the FXO voice port will automatically shut down and restart to allocate or deallocate the DSP voice channel—provided the FXO port is in the Idle state.

Voice-feature configuration commands for a CLI add-on Feature Template

Details CLI commands for configuring and customizing caller ID features on Cisco voice ports using a Feature Template, including alerting methods, blocking, formatting, and DTMF codes, with configuration examples for both FXS and FXO ports.

This section describes how to use specific CLI commands to enable and customize caller ID features for Cisco voice features.

These commands provide configuration options for caller ID features:

- **caller-id alerting dsp-pre-allocate**: Statically allocates a digital signal processor (DSP) voice channel for receiving caller ID information for an on-hook (Type 1) caller ID at a receiving FXO voice port.
- **caller-id alerting line-reversal**: Sets the line-reversal alerting method for caller ID information for an on-hook (Type 1) caller ID at a sending FXS voice port and for an on-hook caller ID at a receiving FXO voice port.
- **caller-id alerting pre-ring**: Sets a 250-millisecond pre-ring alerting method for caller ID information for an on-hook (Type 1) caller ID at a sending FXS and a receiving FXO voice port.
- **caller-id alerting ring**: Sets the ring-cycle method for receiving caller ID information for an on-hook (Type 1) caller ID at a receiving FXO or a sending FXS voice port.
- **caller-id block**: Requests blocking of caller ID information display at the far end of a call that originates from an FXS port.
- **caller-id format e911**: Specifies the caller ID message type that should be the enhanced 911 format for calls that are sent on FXS voice ports.
- **caller-id mode**: Specifies a noncountry, standard caller ID mode for a receiving FXO or a sending FXS voice port.
- **clid dtmf-codes**: Specifies global caller ID DTMF start, redirect, and end codes.

Examples of Adding Voice Features with a CLI Add-On Feature Template

The following example shows caller ID configuration for FXS ports:

```
voice service pots
clid dtmf-codes ABC
!
voice-port 1/0/0
caller-id enable
caller-id alerting ring 3
station name West Wing
station number 4085550100
!
voice-port 1/0/1
caller-id enable
caller-id mode DTMF start * end #
caller-id alerting line-reversal
station name East Wing
station number 4085550101
!
voice-port 1/0/2
caller-id enable
caller-id mode BT
caller-id alerting pre-ring
station name Jose
station number 4085550102
!
voice-port 1/0/3
caller-id enable
caller-id block
station name a-sample
station number 4085552000
!
voice-port 1/0/4
caller-id enable
caller-id format e911
station name sample-2
station number 4085552222
```

The following example shows caller ID configuration for FXO ports:

```
voice service pots
clid dtmf-codes ABC
!
voice-port 2/0/0
cptone BR
caller-id enable
caller-id alerting line-reversal
caller-id alerting dsp-pre-allocate
!
voice-port 2/0/1
caller-id enable
caller-id alerting ring 2
!
voice-port 2/0/2
caller-id enable
caller-id BT FSK
caller-id alerting pre-ring
```

6 Cisco unified border element

Topics:

- Feature history for Cisco unified border element
- Cisco unified border elements (CUBE)
- Supported devices for CUBE configuration
- Restrictions for CUBE configuration
- Use cases for CUBE
- Configure CUBE
- CUBE commands
- SRST commands

Describes the Cisco Unified Border Element (CUBE), a comprehensive session border controller that provides secure SIP and H.323 connectivity between enterprise networks and service provider networks while offering call admission control, security, and protocol interworking capabilities.

Feature history for Cisco unified border element

Provides the feature history and release information for Cisco Unified Border Element functionality.

This reference lists the feature history for Cisco Unified Border Element (CUBE) and related voice functionality, including release information and descriptions of each feature enhancement.

Table 64: Feature history

Feature Name	Release Information	Description
Cisco Unified Border Element (CUBE)	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	Cisco Unified Border Element (CUBE) interconnects voice and video connectivity between VoIP networks. It enables enterprise voice networks to communicate with Internet telephony service providers (ITSPs) and provides Session Border Controller (SBC) functionalities.
Secure SRST Support on Cisco Catalyst SD-WAN	Cisco IOS XE Catalyst SD-WAN Release 17.10.1a Cisco vManage Release 20.10.1	Secure SRST Support on Cisco Catalyst SD-WAN allows you to configure Cisco Survivable Remote Site Telephony (SRST) commands and additional Cisco Unified Border Element (CUBE) commands. Using these commands within Cisco IOS XE Catalyst SD-WAN devices, you can: • Maintain voice services at remote sites during network outages. • Extend advanced voice and video connectivity within Cisco Catalyst SD-WAN You can configure these commands onCisco IOS XE Catalyst SD-WAN devices using Cisco SD-WAN Manager device CLI templates or CLI add-on feature templates.
Supported Voice and SIP-UA Commands	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a Cisco Catalyst SD-WAN Manager Release 20.14.1	This feature provides support for specific commands that enhance voice and SIP-UA functionalities on Cisco IOS XE Catalyst SD-WAN devices. These commands include: • **cipher (voice class)** • **nat media-keepalive** • **secure-ciphersuite** • **transport tcp tls (SIP-ua)** • **voice-class SIP nat media-keepalive**

Feature Name	Release Information	Description
Survivable Remote Site Telephony (SRST) commands	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a Cisco Catalyst SD-WAN Manager Release 20.14.1	This feature provides support for specific commands related to secure HTTP client communication and `call-manager-fallback` transport. These commands include: • **HTTP client secure-ciphersuite** • **transport-tcp-tls (call-manager-fallback)**

Cisco unified border elements (CUBE)

Describes Cisco Unified Border Elements (CUBE), their role as Session Border Controllers (SBCs), and how they enable secure voice and video communication.

A Cisco Unified Border Element (CUBE) is a network device or software that

- facilitates voice and video connectivity between different Voice over IP (VoIP) networks
- primarily functions as a Session Border Controller (SBC), enabling communication between enterprise networks and Internet telephony service providers (ITSPs)
- replaces physical voice trunks with IP-based voice trunks, allowing direct connection to other VoIP networks and ITSPs, and
- provides conventional SBC functions along with a wide variety of advanced features to manage and secure VoIP sessions.

Configuration

You can configure CUBE functionality on Cisco IOS XE Catalyst SD-WAN device using device CLI templates or CLI add-on feature templates.

For more information about CUBE setup, functionality, usage, configuration, and related topics, see the Cisco Unified Border Element Configuration Guide.

Supported devices for CUBE configuration

Lists the devices that support CUBE configuration including Cisco integrated services routers and edge platforms.

This reference provides a comprehensive list of Cisco devices that support CUBE (Cisco Unified Border Element) configuration capabilities.

- Cisco 1000 Series Integrated Services Routers
- Cisco 4000 Series Integrated Services Routers
- Cisco Catalyst 8200 Series Edge Platforms
- Cisco Catalyst 8300 Series Edge Platforms
- Cisco Catalyst 8000v Software Router
- Cisco ASR 1001-X Router

- Cisco ASR 1002-X Router
- Cisco ASR 1006-X Router with the Cisco ASR1000-RP3 Module, and the Cisco ASR1000-ESP100 or ASR1000-ESP100-X Embedded Services Processor
- Cisco ASR 1004 Router with the RP2 Route Processor and the Cisco ASR 1000-ESP40 Embedded Services Processor
- Cisco ASR 1006 Router with the RP2 Route Processor and the Cisco ASR 1000-ESP40 Embedded Services Processor
- Cisco ASR 1006-X Router with the RP2 Route Processor and the Cisco ASR 1000-ESP40 Embedded Services Processor

Supported devices starting from Cisco IOS XE Catalyst SD-WAN Release 26.2.1.

- Cisco 8300 Series Secure Routers–C8375-E-G2 and C8355-G2
- Cisco 8200 Series Secure Routers–C8235-E-G2, C8235-G2, C8231-E-G2, and C8231-G2

Restrictions for CUBE configuration

Describes the limitations for configuring Cisco Unified Border Element, specifically that high-availability configuration is not supported in CUBE deployments.

High-availability configuration is not supported for CUBE.

Starting with Cisco IOS XE Catalyst SD-WAN Release 26.2.1, CUBE support is limited to deployments without vDSP, high availability (HA), or TDM cards. CUBE must be configured using a Cisco SD-WAN Manager device CLI template or CLI add-on feature template.

Use cases for CUBE

Lists the various applications where CUBE can configure SBC elements for enterprise and cloud communication solutions.

CUBE can configure SBC elements for various applications, such as:

- Enterprise Premises-Based Collaboration: using Cisco Unified Communications Manager (or another call control application) with centralized or local PSTN breakouts.
- Local Breakout Gateway for Cisco Unified Communications Manager Cloud: a Cisco-hosted cloud service for large enterprises.
- Local Gateway to Enable the Bring Your Own PSTN (BYoPSTN) Option for Cisco Webex Calling: to enable the Bring Your Own PSTN (BYoPSTN) option.
- Edge Audio for Cisco Webex Meetings: with a direct VoIP route to the Cisco Webex cloud or through existing PSTN services.

Configure CUBE

Configure CUBE functionality on a device by creating a Cisco IOS XE Catalyst SD-WAN device CLI template or CLI add-on feature template.

This task guides you on how to configure CUBE functionality on a device.

CUBE (Cisco Unified Border Element) enables devices to process voice and video traffic with proper call routing and media handling capabilities.

Before you begin

Create a Cisco IOS XE Catalyst SD-WAN device CLI template or a CLI add-on feature template for the device to use the CUBE functionality

Follow these steps to configure CUBE:

Procedure

Create a Cisco IOS XE Catalyst SD-WAN device CLI template or a CLI add-on feature template for the device to use the CUBE functionality

Example

The following example shows a basic CUBE configuration using a CLI add-on template:

```
voice service voip
 ip address trusted list
  ipv4 10.0.0.0.255.0.0.0
  ipv6 2001:DB8:0:ABCD::1/48
  !
 allow-connections sip to sip
 sip
  no call service stop
  !
dial-peer voice 100 voip
  description Inbound LAN side dial-peer
  session protocol sipv2
  incoming called number .T
  voice-class codec 1
  dtmf-relay rtp-nte
  !
 dial-peer voice 101 voip
  description Outbound LAN side dial-peer
  destination pattern [2-9].........
  session protocol sipv2
  session target ipv4:10.10.10.1
  voice-class codec 1
  dtmf-relay rtp-nte
  !
 dial-peer voice 200 voip
  description Inbound WAN side dial-peer
  session protocol sipv2
  incoming called-number .T
  voice-class codec 1
  dtmf-relay rtp-nte
  !
 dial-peer voice 201 voip
  description Outbound WAN side dial-peer
  destination pattern [2-9].........
  session protocol sipv2
  session target ipv4:20.20.20.1
  voice-class codec 1
  dtmf-relay rtp-nte
```

For information about device CLI templates and CLI add-on templates, refer to the *Cisco Catalyst SD-WAN Control Components and Device Management Guide*.

For information about CUBE configuration and usage, refer to the Cisco Unified Border Element Configuration Guide.

For information about the CUBE commands that Cisco Catalyst SD-WAN supports for use in a CLI template, refer to CUBE commands on page 142 .

After successfully applying the configuration, the device is enabled to function as a Cisco Unified Border Element, processing voice and video traffic according to the defined dial-peers and voice service settings.

What to do next

After configuring CUBE, you should verify the voice service and dial-peer configurations to ensure proper call routing and media handling. You can also integrate the CUBE-enabled device with your Cisco Unified Communications Manager or other call control applications. For more information, refer to Verify CUBE on the Device.

CUBE commands

Outlines supported CLI template commands for CUBE configuration in Cisco Catalyst SD-WAN, providing links to details on each command's syntax, usage, and configuration options across signaling, media, security, call processing, and SIP-specific settings.

The following table lists the commands that are supported by Cisco Catalyst SD-WAN CLI templates for CUBE configuration. Click a command name in the Command column to view information about the command, its syntax, and its use.

> **Note**
>
> Some configurations and protocols are identified as insecure and is a security risk for Cisco devices. Existing deployments continue to function, but new installations require intentional enablement. For more information on remediation, refer to Resilient Infrastructure: Cisco Catalyst SD-WAN and Routing

Table 65: Cisco Catalyst SD-WAN CLI template commands for CUBE configuration

Command	Description
address-hiding	Hides signaling and media peer addresses from endpoints other than the gateway.
anat	Enables Alternative Network Address Types (ANAT) on a SIP trunk.
answer-address	Specifies the full E.164 telephone number to be used to identify the dial peer of an incoming call.
application (global)	Enters application configuration mode to configure applications.
asserted-id	Enables support for the asserted ID header in incoming SIP requests or response messages, and to send the asserted ID privacy information in outgoing SIP requests or response messages.
asymmetric payload	Configures SIP asymmetric payload support.
audio forced	Allows only audio and image (for T.38 Fax) media types, and drops all other media types).
authentication	Enables SIP digest authentication.
bind	Binds the source address for signaling and media packets to the IPv4 or IPv6 address of a specific interface.
block	Configures global settings to drop (not pass) specific incoming SIP provisional response messages on a CUBE.

Command	Description
call spike	Configures the limit on the number of incoming calls received in a short period (a call spike).
call threshold global	Enables the global resources of a gateway.
call treatment action	Configures the action that the router takes when local resources are unavailable.
call treatment cause-code	Specifies the reason for the disconnection to the caller when local resources are unavailable.
call treatment isdn-reject	Specifies the rejection cause code for ISDN calls when all ISDN trunks are busied out, but the switch ignores the busyout trunks and still sends ISDN calls into the gateway.
call treatment on	Enables call treatment to process calls when local resources are unavailable.
callmonitor	Enables the call monitoring messaging functionality on a SIP endpoint in a VoIP network.
call-route	Enables header-based routing at the global configuration level.
cipher (voice class)	Configures the cipher setting, and associates it to a TLS profile.
clid	Passes the network-provided ISDN numbers in an ISDN calling party information element screening indicator field, and removes the calling party name and number from the calling-line identifier in voice service voip configuration mode. Alternatively, allows the presentation of the calling number by substituting for the missing **Display Name** field in the Remote-Party-ID and From headers.
codec preference	Specifies a list of preferred codecs to use on a dial peer.
codec profile	Defines audio and video capabilities that are needed for video endpoints.
codec transparent	Enables codec capabilities to be passed transparently between endpoints in a CUBE.
conn-reuse	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a . Reuses the TCP connection of a SIP registration for an endpoint behind a firewall.
connection-reuse	Uses global listener port for sending requests over UDP.
contact-passing	Configures pass-through of the contact header from one leg to the other leg for 302 pass-through.
cpa	Enables the call progress analysis (CPA) algorithm for outbound VoIP calls and to set CPA parameters.
credentials	Configures a SIP TDM gateway or CUBE to send a SIP registration message when in the UP state.
crypto signaling	Identifies the **trustpoint** *trustpoint-name* keyword and argument that is used during the Transport Layer Security (TLS) handshake that corresponds to the remote device address.

Command	Description
dial-peer cor custom	Specifies that named class of restrictions (COR) apply to dial peers.
dial-peer cor list	Defines a class of restrictions (COR) list name.
disable-early-media 180	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a . Specifies which call treatment, early media or local ringback, is provided for 180 responses with 180 responses with Session Description Protocol (SDP).
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.
dtmf-interworking	Enables a delay between the dtmf-digit begin and dtmf-digit end events in the RFC 2833 packets sent from CUBE, and generates RFC 4733 compliance RTP Named Telephony Event (NTE) packets from CUBE.
early-media update block	Blocks the UPDATE requests with the Session Description Protocol (SDP) in an early dialog.
early-offer	Forces CUBE to send a SIP invite with Early Offer on the Out Leg.
emergency	Configures a list of emergency numbers.
error-code-override	Configures the SIP error code to be used at the dial peer.
error-passthru	Enables the passage of error messages from the incoming SIP leg to the outgoing SIP leg.
g729-annexb override	Configures the settings for G.729 codec interoperability and overrides the default value if the annexb attribute is not present.
gcid	Enables Global Call ID (GCID) for every call on an outbound leg of a VoIP dial peer for a SIP endpoint.
gw-accounting	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a . Enables an accounting method for collecting call detail records (CDRs).
handle-replaces	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a . Configures a Cisco IOS device to handle SIP INVITE with Replaces header messages at the SIP protocol level.
header-passing	Enables the passing of headers to and from SIP INVITE, SUBSCRIBE, and NOTIFY messages.
host-registrar	Populates the sip-ua registrar domain name or IP address value in the host portion of the diversion header and redirects the contact header of the 302 response.
http client connection idle timeout	Sets the number of seconds for which the HTTP client waits before terminating an idle connection.
http client connection persistent	Enables HTTP persistent connections so that multiple files can be loaded by using the same connection.

Command	Description
http client connection timeout	Sets the number of seconds for which the HTTP client waits for a server to establish a connection before abandoning its connection attempt.
ip qos dscp	Configures the DSCP value for QoS.
localhost	Globally configures CUBE to substitute a DNS hostname or domain as the localhost name in place of the physical IP address in the From, Call-ID, and Remote-Party-ID headers in outgoing messages.
max-conn	Specifies the maximum number of incoming or outgoing connections for a particular VoIP dial peer.
max-forwards	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a . Globally sets the maximum number of hops, that is, proxy or redirect servers that can forward the SIP request.
media	Enables media packets to pass directly between endpoints without the intervention of CUBE, and enables signaling services.
media disable-detailed-stats	Disables the collection of detailed call statistics.
media profile asp	Creates a media profile to configure acoustic shock-protection parameters.
media profile nr	Creates a media profile to configure noise-reduction parameters.
media profile stream-service	Enables stream service on CUBE.
media profile video	Creates a media profile video.
media-address voice-vrf	Associates an RTP port range with VRF.
media-inactivity-criteria	Specifies the mechanism for detecting media inactivity (silence) on a voice call.
midcall-signaling	Configures the method that is used for signaling messages.
min-se	Changes the minimum session expiration (Min-SE) header value for all the calls that use the SIP session timer.
nat	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a . Uses SIP Network Address Translation (NAT) global configuration.
nat media-keepalive	Enables media keepalive packet transmission for the specified interval of time.
notify redirect	Enables application handling of redirect requests for all VoIP dial peers.
notify ignore substate	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a . Specifies Ignoring the Subscription-State header in a Notify message.
notify telephone-event	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a . Configures the maximum interval between two consecutive NOTIFY messages for a particular telephone event.

Command	Description
num-exp	Defines how to expand a telephone extension number into a particular destination pattern.
options-ping	Enables in-dialog options.
outbound-proxy	Configures a SIP outbound proxy for outgoing SIP messages globally.
pass-thru content	Enables the pass-through of SDP from in-leg to the out-leg.
permit hostname	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a . Stores hostnames used during validation of initial incoming INVITE messages.
privacy	Sets privacy support at the global level as defined in RFC 3323.
privacy-policy	Configures the privacy header policy options at the global level.
progress_ind	Configures an outbound dial peer on a CUBE to override and remove or replace the default progress indicator in specified call messages.
protocol mode	Configures the Cisco IOS SIP stack.
random-contact	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a . Populates an outgoing INVITE message with random-contact information instead of clear-contact information.
reason-header override	Enables cause code passing from one SIP leg to another.
redirect ip2ip	Redirects SIP phone calls to SIP phone calls globally on a gateway.
redirection	Enables the handling of 3 *xx* redirect messages
referto-passing	Disables dial peer lookup and modification of the Refer-To header when the CUBE passes across a REFER message during a call transfer.
registrar	Enables SIP gateways to register E.164 numbers on behalf of analog telephone voice ports (FXS), IP phone virtual voice ports (EFXS), and SCCP phones with an external SIP proxy or SIP registrar.
rel1xx	Enables SIP provisional responses (other than 100 Trying) to be sent reliably to the remote SIP endpoint.
remote-party-id	Enables translation of the Remote-Party-ID SIP header.
requri-passing	Enables pass-through of the host part of the Request-URI and To SIP headers.
retry bye	Configures the number of times that a BYE request is retransmitted to the other user agent.
retry invite	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a . Configures the number of times that a SIP INVITE request is retransmitted to the other user agent.
rtcp all-pass-through	Passes through all the RTCP packets in the datapath.

Command	Description
rtcp keepalive	Configures RTCP keepalive report generation and generates RTCP keepalive packets.
rtp payload-type	Identifies the payload type of an RTP packet.
rtp-media-loop count	Configures the number of media loops before RTP voice and video media packets are dropped.
rtp-port	Configures the real-time protocol range.
rtp-ssrc multiplex	Multiplexes RTCP packets with RTP packets and sends multiple synchronization source in RTP headers (SSRCs) in an RTP session.
secure-ciphersuite	Configures the cipher suites (encryption algorithms) to be used for encryption over HTTPS for a WebSocket connection in CUBE.
session refresh	Enables SIP session refresh globally.
session transport	Configures a VoIP dial peer to use TCP or UDP as the underlying transport layer protocol for SIP messages.
set pstn-cause	Maps an incoming PSTN cause code to a SIP error status code.
set sip-status	Maps an incoming SIP error status code to a PSTN cause code.
signaling forward	Configures global settings for transparent tunneling of QSIG, Q.931, H.225, and ISUP messages.
silent discard untrusted	Discards SIP requests from untrusted sources in an incoming SIP trunk.
sip-server	Configures a network address for the SIP server interface.
srtp	Specifies that SRTP be used to enable secure calls and call fallback.
srtp negotiate	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a . Enables the Cisco IOS Session Initiation Protocol (SIP) gateway to accept and send a Real-Time Transport Protocol (RTP) Audio/Video Profile (AVP) at the global configuration level.
stun	Enters STUN configuration mode for configuring firewall traversal parameters.
stun flowdata shared-secret	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a . Configures a secret shared on a call control agent.
stun usage firewall-traversal flowdata	Enables firewall traversal using STUN.
supplementary-service media-renegotiate	Globally enables midcall media renegotiation for supplementary services.
timers	Configures SIP-signaling timers.
transport	Configures the SIP user agent (gateway) for SIP signaling messages in inbound calls through the SIP TCP, TLS over TCP, or UDP socket. This command supports TLS version 1.3 and all associated ciphers.

Command	Description
uc secure-wsapi	Configures a secure Cisco Unified Communication IOS services environment for a specific application.
uc wsapi	Configures a nonsecure Cisco Unified Communication IOS services environment for a specific application.
update-callerid	Enables sending updates for caller IDs.
url (SIP)	Configures URLs to either the SIP, SIP secure (SIPS), or telephone (TEL) format for your VoIP SIP calls.
vad	Enables VAD for calls using a specific dial peer.
video codec	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a .
voice cause code	Sets the internal Q850 cause code mapping for, voice and enters voice cause configuration mode.
voice class codec	Enters voice-class configuration mode and assigns an identification tag number for a codec voice class.
voice class dpg	Creates a dial-peer group for grouping multiple outbound dial peers.
voice class e164-pattern-map	Creates an E.164 pattern map that specifies multiple destination E.164 patterns in a dial peer.
voice class media	Configures media control parameters for voice.
voice class server-group	Enters voice-class configuration mode and configures server groups (groups of IPv4 and IPv6 addresses) that can be referenced from an outbound SIP dial peer.
voice-class sip options-keepalive	Monitors connectivity between CUBE VoIP dial peers and SIP servers.
voice class sip-copylist	Configures a list of entities to be sent to the peer call leg.
voice class sip-event-list	Configures a list of SIP events to be passed through.
voice class sip-hdr-passthrulist	Configures a list of headers to be passed through the route string.
voice-class sip nat media-keepalive	Configures media keepalive to enable media keepalive packets to be transmitted for the interval specified.

voice class sip-profiles	Configures SIP profiles for a voice class.
	Configuring a sip profile, **request REGISTER sip-header Authorization modify "550\"," [550@dl.ims.airtel.in|mailto:550@dl.ims.airtel.in]"** , on a device throws a warning message:
	`Device# show run`
	`sec sip-profiles voice class sip-profiles 4 rule 2`
	`request REGISTER sip-header Authorization modify`
	`"550\","`
	`"[550@dl.ims.airtel.in|mailto:550@dl.ims.airtel.in]""`

Command	Description
voice class srtp-crypto	Enters voice class configuration mode and assigns an identification tag for an **srtp-crypto voice class** command.
voice class uri	Creates or modifies a voice class for matching dial peers to a SIP or TEL URI.
voice class tls-cipher	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a . Configures an ordered set of TLS cipher suites.
voice class tls-profile	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a . Enables voice class configuration mode, and assigns an identification tag for a TLS profile.
voice iec syslog	Enables viewing of internal error codes as they are encountered in real time.
voice statistics iec	Enables collection of internal error code statistics.
xfer target	Minimum supported releases: Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a . Routes the INVITE to the refer-to destination in the REFER consume case. The routing decision is made based on the xfer target destination.

SRST commands

Lists the commands that are supported by Cisco Catalyst SD-WAN CLI templates for SRST.

This table lists the commands that are supported by Cisco Catalyst SD-WAN CLI templates for SRST. Click a command name in the Command column to view information about the command, its syntax, and its use.

Table 66: Cisco Catalyst SD-WAN CLI template commands for SRST

Command	Description
HTTP client secure-ciphersuite	Sets the secure encryption cipher suite for the HTTP client.
transport-tcp-TLS (call-manager-fallback)	Configures a specific TLS version for Unified Secure SCCP SRST, in call-manager-fallback mode.

7 Onboarding ThousandEyes Agent and Onboarding Tests

Topics:

- Feature History for Simplified Onboarding of Cisco ThousandEyes Agent
- Onboarding Cisco ThousandEyes agents and configuring tests
- Create an IP pool for the Cisco ThousandEyes agents
- Prerequisites for simplified workflow
- Restrictions for simplified workflow
- Configure Cisco ThousandEyes agent and tests using simplified workflow
- Monitor onboarded Cisco ThousandEyes agents and configured tests
- Troubleshoot Cisco ThousandEyes agent on edge device

Feature History for Simplified Onboarding of Cisco ThousandEyes Agent

Outlines the feature history of simplified onboarding for Cisco ThousandEyes Agent, detailing its release versions and describing the streamlined workflow for onboarding the agent and configuring tests.

This table describes the developments of this feature, by release.

Table 67: Feature History

Feature Name	Release Information	Feature Description
Simplified Workflow for Onboarding Cisco ThousandEyes Agent and Configuring Tests	Cisco IOS XE Catalyst SD-WAN Release 17.16.1a Cisco Catalyst SD-WAN Manager Release 20.16.1	A simplified workflow to easily onboard Cisco ThousandEyes agent and configure tests using Cisco SD-WAN Manager.

Onboarding Cisco ThousandEyes agents and configuring tests

Describes a simplified workflow for onboarding Cisco ThousandEyes agents and configuring application monitoring tests directly from Cisco SD-WAN Manager.

Summary

The key components involved in onboarding Cisco ThousandEyes agents and configuring tests are:

- Cisco SD-WAN Manager: Provides the central interface for establishing connections, configuring tests, and monitoring
- Cisco ThousandEyes platform: Hosts the agents and executes the application monitoring tests
- ThousandEyes agents: Perform the actual testing and monitoring of applications
- Applications, sites, and devices: The targets for testing and monitoring activities

Workflow

These are the stages of onboarding Cisco ThousandEyes agents and configuring tests:

1. Establish a connection to the Cisco ThousandEyes platform through SD-WAN Manager.
2. Configure tests in Cisco ThousandEyes directly from SD-WAN Manager.
3. Choose applications, sites, and devices for testing and configure the necessary parameters in SD-WAN Manager.
4. Monitor the agents and tests from the **ThousandEyes Monitoring** dashboard in SD-WAN Manager.

Create an IP pool for the Cisco ThousandEyes agents

Configure an IP pool specifically for Cisco ThousandEyes agents to enable network monitoring capabilities.

Create a dedicated IP pool that provides network addresses for Cisco ThousandEyes agents, enabling them to perform network monitoring and testing functions within your SD-WAN environment.

This section describes the procedure of onboarding Cisco ThousandEyes agent. You need to configure a specialized IP pool that will be used exclusively by ThousandEyes agents for network monitoring operations.

Procedure

1. From the menu, choose **Configuration** > **Network Hierarchy**.

   Note

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

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

The IP pool for Cisco ThousandEyes agents is created and available for use in network monitoring operations.

What to do next

- Monitor the status of agents and enable or disable agents in the **ThousandEyes Monitoring** dashboard in the Cisco SD-WAN Manager.
- Launch **ThousandEyes Monitoring** dashboard to view test results.

Prerequisites for simplified workflow

Lists the tasks you must complete before initiating the simplified workflow to onboard Cisco ThousandEyes agent and configure tests.

You must complete the tasks in this section before initiating the simplified workflow.

Table 68: Tasks before running the simplified workflow

Configuration Task	Information
Deploy Cisco IOS XE Catalyst SD-WAN devices using the configuration group.	Refer to Deploy Devices Using the Deploy Configuration Group Workflow.
Upload Cisco ThousandEyes Enterprise agent software.	• To upload software on the SD-WAN Manager software repository, refer to Upload the Cisco ThousandEyes Enterprise Agent software to SD-WAN Manager. • To add virtual images from a remote server, refer to the Add Virtual Images to the Repository section in the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*.

Configuration Task	Information
Create an IP pool in the global node of Network Hierarchy Manager. When deploying Cisco ThousandEyes agent through the workflow, the Virtual Port Group Interface IP address contains this IP pool.	Refer to Create an IP pool for the Cisco ThousandEyes agents on page 152.
Add IPv4 DNS server details in the Transport VPN feature of the Configuration Group associated with the device.	Refer to DNS.

Restrictions for simplified workflow

Outlines the limitations and requirements when using the simplified workflow for Cisco ThousandEyes Agent deployment and configuration.

Minimum supported releases: Cisco Catalyst SD-WAN Manager Release 20.16.1 and Cisco IOS XE Catalyst SD-WAN Release 17.16.1a

Editing limitations for deployed ThousandEyes agent sites

The workflow does not support editing tests or updating agent parameters for sites with deployed Cisco ThousandEyes agents.

Workflow only supports devices with configuration groups

The simplified workflow supports only devices that are associated with configuration groups.

Workflow only supports one device in a site

The simplified workflow supports only devices associated with configuration groups. In the workflow, you can select only one device in a site to deploy the Cisco ThousandEyes Agent and configure tests associated with it. To deploy Cisco ThousandEyes Agent on multiple devices in a site, use the Configuration Group method, see Using Configuration Groups.

Configure Cisco ThousandEyes agent and tests using simplified workflow

Configure Cisco ThousandEyes agents and monitoring tests directly from Cisco SD-WAN Manager using the simplified workflow.

This task enables you to onboard Cisco ThousandEyes agents and configure monitoring tests directly from the SD-WAN Manager using a streamlined workflow process.

The simplified workflow provides an integrated approach to configure Cisco ThousandEyes monitoring within your SD-WAN environment, eliminating the need to manage agents and tests separately across multiple platforms.

Before you begin

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.16.1 and Cisco IOS XE Catalyst SD-WAN Release 17.16.1a

- Ensure the following before initiating the simplified workflow:
  - You have a Cisco ThousandEyes account before using the simplified workflow to configure a Cisco ThousandEyes agent in Cisco SD-WAN Manager.
  - You must be a user with the Organization Admin role to access the Cisco ThousandEyes account.
- Create an IP pool in the global node of Network Hierarchy Manager, see Create an IP pool for the Cisco ThousandEyes agents on page 152.

Follow these steps to configure Cisco ThousandEyes agent and tests using the simplified workflow:

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Workflows** > **Workflow Library**.
2. Start the **Configure ThousandEyes** workflow.
3. Read the terms and conditions. After accepting the terms and conditions, click **Connect ThousandEyes** to start the workflow.
4. When the Cisco ThousandEyes portal opens, log in to your account using your login credentials. The page redirects to Cisco SD-WAN Manager.
5. Follow the instructions provided in the workflow.

> **Note**
>
> - In the workflow, select all sites associated with a specific Configuration Group simultaneously. This ensures that the Configuration Group with Cisco ThousandEyes agent applies to all sites associated with the Configuration Group.
> - The time required to onboard Cisco ThousandEyes agent and configure tests varies based on the size of your network.

The Cisco ThousandEyes agents are onboarded and monitoring tests are configured in your SD-WAN environment using the simplified workflow.

What to do next

- Monitor the status of agents and enable or disable agents in the **ThousandEyes Monitoring** dashboard in the Cisco SD-WAN Manager.
- Launch **ThousandEyes Monitoring** dashboard to view test results.

Monitor onboarded Cisco ThousandEyes agents and configured tests

Configure monitoring of Cisco ThousandEyes agents and tests using the monitoring dashboard in SD-WAN Manager.

You can monitor the status of Cisco ThousandEyes agents and configured tests in the SD-WAN Manager.

This task helps you track the operational status of your ThousandEyes deployment and view configured tests through the monitoring dashboard interface.

Before you begin

Ensure you are on release Cisco Catalyst SD-WAN Manager Release 20.16.1 and Cisco IOS XE Catalyst SD-WAN Release 17.16.1a.

Follow these steps to monitor onboarded Cisco ThousandEyes agents and configured tests:

Procedure

1. To monitor the status of Cisco ThousandEyes agents and configured tests in the SD-WAN Manager monitoring dashboard, navigate to **Tools** > **ThousandEyes Monitoring**.

   You can view the online, offline, and disabled agents, and launch Cisco ThousandEyes from the dashboard.

2. In the monitoring dashboard, review these sections:
   - **Tests**: View information about the tests configured using the simplified workflow.
   - **Agents**: View information about the status of Cisco ThousandEyes agents configured using the simplified workflow. It also provides a list of configured devices and sites for the test with the option to enable, disable, or delete a Cisco ThousandEyes agent.

You can now view the status of all ThousandEyes agents and tests, including online, offline, and disabled agents, through the monitoring dashboard interface.

Troubleshoot Cisco ThousandEyes agent on edge device

Configure troubleshooting procedures to identify and resolve issues with the Cisco ThousandEyes agent on edge devices.

This task helps you identify and resolve issues with the Cisco ThousandEyes agent deployment on edge devices by examining relevant log files and audit logs.

Use this troubleshooting procedure when experiencing problems with Cisco ThousandEyes agent functionality on edge devices, such as failed test configurations or agent communication issues.

Before you begin

Ensure you are on release Cisco Catalyst SD-WAN Manager Release 20.16.1 and Cisco IOS XE Catalyst SD-WAN Release 17.16.1a.

Follow these steps to troubleshoot Cisco ThousandEyes agent issues on edge devices:

Procedure

1. Review these log files in SD-WAN Manager for error messages or relevant information: /var/log/nms/vmanage-server.log and /var/log/nms/vmanage-server-deviceconfig-template.log.
2. Examine the audit logs to determine if the ThousandEyes test was posted or it failed.

You have reviewed the relevant log files and audit logs to identify any issues with the Cisco ThousandEyes agent configuration or test deployment on the edge device.

8 Monitoring with Cisco ThousandEyes

Topics:

- Feature history for extended visibility with Cisco Catalyst SD-WAN and ThousandEyes
- Extending visibility for Cisco Catalyst SD-WAN and Cisco ThousandEyes
- Supported devices for running Cisco SD-WAN and Cisco ThousandEyes
- ThousandEyes enterprise agent supported versions and system requirements
- Prerequisites for extending visibility with SD-WAN manager and Cisco ThousandEyes
- Restrictions for extending visibility with SD-WAN manager and Cisco ThousandEyes
- Configure a Cisco ThousandEyes enterprise agent using a configuration group
- Upload the Cisco ThousandEyes Enterprise Agent software to SD-WAN Manager
- Provision Cisco ThousandEyes Enterprise Agent in a Service VPN or Transport VPN (VPN0)
- Provision a Cisco ThousandEyes enterprise agent in a service VPN using CLI
- Uninstall the Cisco ThousandEyes enterprise agent software
- Upgrade the Cisco ThousandEyes enterprise agent software
- Troubleshoot the Cisco ThousandEyes Enterprise Agent on Cisco IOS XE Catalyst SD-WAN devices

Feature history for extended visibility with Cisco Catalyst SD-WAN and ThousandEyes

Outlines the feature history for extended visibility with Cisco Catalyst SD-WAN and ThousandEyes, including deployment options, integration processes, release information, expanded device support for Enterprise Agent, and enhanced network and application performance monitoring capabilities.

The feature history table provides information about when specific features were introduced.

Table 69: Feature History

Feature Name	Release Information	Description
Extended Visibility with Cisco Catalyst SD-WAN and Cisco ThousandEyes	Cisco IOS XE Release 17.6.1a Cisco vManage Release 20.6.1	You can deploy Cisco ThousandEyes Enterprise agent natively as a container application on supported Cisco IOS XE Catalyst SD-WAN devices to integrate Cisco Catalyst SD-WAN with Cisco ThousandEyes. You can install and activate the Cisco ThousandEyes Enterprise agent through SD-WAN Manager. By integrating Cisco Catalyst SD-WAN with Cisco ThousandEyes, you can gain granular insights into network and application performance with full hop-by-hop path analysis across the Internet, and isolate fault domains for expedited troubleshooting and resolution.
Cisco ThousandEyes Support for Cisco 1000 Series Integrated Services Routers	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	You can deploy Cisco ThousandEyes Enterprise agent natively as a container application on Cisco ISR 1100X-6G devices. You can install and activate the Cisco ThousandEyes Enterprise agent through SD-WAN Manager.
Cisco ThousandEyes Support for Cisco Catalyst 8500 Series Edge Platforms and Cisco ASR 1000 Series Aggregation Services Routers	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1	You can deploy Cisco ThousandEyes Enterprise agent natively as a container application on Cisco Catalyst 8500 Series Edge Platforms and Cisco ASR 1000 Series Aggregation Services Routers. You can install and activate the Cisco ThousandEyes Enterprise agent through SD-WAN Manager.
Extended Device Support for the Cisco ThousandEyes Agent in Cisco ISR 1100 Series	Cisco IOS XE Catalyst SD-WAN Release 17.16.1a Cisco Catalyst SD-WAN Manager Release 20.16.1	Support for the Cisco ThousandEyes Enterprise agent is extended to additional routers in Cisco ISR 1100 Series.
Extended Device Support for the Cisco ThousandEyes Agent to Industrial Routers	Cisco IOS XE Catalyst SD-WAN Release 17.18.2 Cisco Catalyst SD-WAN Manager Release 20.18.2	Support for the Cisco ThousandEyes Enterprise Agent is extended to include industrial routers in SD-WAN deployments.

Extending visibility for Cisco Catalyst SD-WAN and Cisco ThousandEyes

Explains how Cisco ThousandEyes extends network visibility for Cisco Catalyst SD-WAN deployments through end-to-end monitoring and real-time performance insights.

Cisco ThousandEyes is a SaaS application that

- delivers end-to-end visibility across internal, external, and carrier networks,
- monitors network performance in real time to provide actionable insights, and
- optimizes application delivery and end-user experience through continuous analysis of network paths and services.

Deploy and configure the ThousandEyes agent

From Cisco IOS XE Release 17.6.1, you can deploy and configure the Cisco ThousandEyes Enterprise agent on Cisco IOS XE Catalyst SD-WAN devices to enable extensive monitoring of the WAN traffic for enhanced visibility within and beyond the Cisco Catalyst SD-WAN fabric. The Cisco ThousandEyes Enterprise agent is an embedded Docker-based application that runs on Cisco IOS XE Catalyst SD-WAN devices as a docker-type container application using the IOX Docker application-hosting capability.

From Cisco Catalyst SD-WAN Manager Release 20.14.1, you can navigate to Cisco services hosted in the Cisco Networking Cloud, such as Cisco ThousandEyes. Enable the cross platform navigator in **Administration** > **Settings** > **Cross Platform Navigator**.

For more information on Cisco ThousandEyes and on configuring tests and viewing results in the Cisco ThousandEyes portal, see the *Cisco ThousandEyes Getting Started* documentation.

Supported devices for running Cisco SD-WAN and Cisco ThousandEyes

Provides Cisco IOS XE Catalyst SD-WAN devices that support deployment of the Cisco ThousandEyes Enterprise agent as a container application.

The table provides Cisco IOS XE Catalyst SD-WAN devices that support deployment of the Cisco ThousandEyes Enterprise agent as a container application.

Platform	Device Model	Architecture	Release
Cisco Catalyst 8300 Series Edge Platforms	C8300-1N1S-6T C8300-1N1S-4T2X C8300-2N2S-6T C8300-2N2S-4T2X	x86_64	Cisco vManage Release 20.6.1 Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and later
Cisco Catalyst 8200 Series Edge Platforms	C8200-1N-4T C8200L-1N-4T	x86_64	
Cisco 4000 Series Integrated Services Routers	ISR4461 ISR4451 ISR4431 ISR4351 ISR4331 ISR4321 ISR4221X	x86_64	
Cisco 1000 Series Integrated Services Routers	ISR1100X-6G	x86_64	Cisco vManage Release 20.7.1 Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and later
Cisco Catalyst 8500 Series Edge Platforms	C8500-12X C8500-12X4QC C8500L-8S4X	x86_64	Cisco vManage Release 20.8.1 Cisco IOS XE Catalyst SD-WAN Release 17.8.1a and later
Cisco ASR 1000 Series Aggregation Services Routers	ASR 1001-HX ASR 1001-X ASR 1002-HX ASR 1002-X ASR 1006-X (RP3)	x86_64	

Platform	Device Model	Architecture	Release
Cisco 1000 Series Integrated Services Routers	C1111X-8P C1121X-8P C1121X-8PLTEP C1121X-8PLTEPW C1126X-8PLTEP C1127X-8PLTEP C1131X-8PW C1131X-8PLTEPW C1161X-8P C1161X-8PLTEP	aarch64	Cisco Catalyst SD-WAN Manager Release 20.16.1 Cisco IOS XE Catalyst SD-WAN Release 17.16.1a
Cisco 8100 Series Secure Routers	C8151-G2 C8161-G2	aarch64	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a
Cisco 8200 Series Secure Routers	C8235-E-G2, C8231-E-G2 C8235-G2 C8231-G2	aarch64	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a
Cisco 8300 Series Secure Routers	C8355-G2 C8375-E-G2	aarch64	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a **Note** C8375-E-G2 is supported from Cisco IOS XE Catalyst SD-WAN 17.15.3
Cisco 8400 Series Secure Routers	C8400-G2	aarch64	Cisco IOS XE Catalyst SD-WAN 17.15.3
Cisco IR1800 Rugged Series Routers	IR1833 IR1835	aarch64	Cisco IOS XE Catalyst SD-WAN Release 17.18.2 Cisco Catalyst SD-WAN Manager Release 20.18.2
Cisco IR1101 Rugged Series Routers	IR1101	aarch64	Cisco IOS XE Catalyst SD-WAN Release 17.18.2 Cisco Catalyst SD-WAN Manager Release 20.18.2

Platform	Device Model	Architecture	Release
Cisco IR8100 Heavy Duty Series Routers	IR8140H IR8140H-P	aarch64	Cisco IOS XE Catalyst SD-WAN Release 17.18.2 Cisco Catalyst SD-WAN Manager Release 20.18.2
Cisco IR8300 Rugged Series Routers	IR8340	x86_64	Cisco IOS XE Catalyst SD-WAN Release 17.18.2 Cisco Catalyst SD-WAN Manager Release 20.18.2
Cisco 8100 Series Secure Routers	C8131-G2 C8151-CVAI-G2 C8151-CVAP-G2	aarch64	Cisco Catalyst SD-WAN Manager Release 26.1.1.1 Cisco IOS XE Catalyst SD-WAN Release 26.1.1

ThousandEyes enterprise agent supported versions and system requirements

Provides system requirements and storage specifications for ThousandEyes Enterprise Agent deployment on Cisco devices.

We recommend you to update to the latest version of the ThousandEyes Enterprise agent. Download the latest version of the ThousandEyes Enterprise agent from the Cisco ThousandEyes Agent page.

Storage and DRAM requirements

- External Storage: On devices that are equipped with external storage (SSD M.2 NVMe), the Cisco ThousandEyes Enterprise agent is installed in the external storage. The minimum external storage capacity that is required to install the Cisco ThousandEyes Enterprise agent is 8 GB. If the device does not have sufficient external storage capacity, upgrade the storage capacity to meet the minimum requirement.

  Although the minimum external storage capacity that is required is 8 GB, we recommend that you provision the device with an external storage capacity of 16 GB or more. With the minimum external storage capacity, you may need to manually clean up files while upgrading the software image on the device.

- Bootflash: On devices that are not equipped with external storage, the Cisco ThousandEyes Enterprise agent is installed on the bootflash. The minimum bootflash capacity that is required to install the Cisco ThousandEyes Enterprise agent is 8 GB. If the device does not have sufficient bootflash capacity, upgrade the storage capacity to meet the minimum requirement.

  Note

  On the ISR1100X-6G, the Cisco ThousandEyes Enterprise agent is installed on the bootflash. For this particular device model, the minimum bootflash capacity that is required to install the agent is 16 GB.

  Although the minimum bootflash capacity that is required is 8 GB, we recommend that you provision the device with an bootflash capacity of 16 GB or more. With the minimum bootflash capacity, you may need to manually clean up files while upgrading the software image on the device.

- DRAM: The minimum DRAM capacity that is required to install the Cisco ThousandEyes Enterprise agent is 8 GB. If a device does not have the minimum DRAM capacity that is required to install the Cisco ThousandEyes Enterprise agent, upgrade the DRAM to meet the minimum requirement.
- Co-residency: Cisco ThousandEyes Enterprise agent can be deployed with other applications if the device has the resources (CPU, memory, and storage) to run the other applications. If the available resources are not sufficient to run the other applications, IOX generates an error message and does not run the other applications.
- To host the Cisco ThousandEyes Enterprise agent, a Cisco IOS XE Catalyst SD-WAN device must have a minimum of 8 GB DRAM. To host additional applications such as UTD and DRE on the same device, provision the device with at least a 16 GB DRAM.

Prerequisites for extending visibility with SD-WAN manager and Cisco ThousandEyes

Lists the requirements needed to extend network visibility using SD-WAN Manager and Cisco ThousandEyes.

To extend network visibility using SD-WAN Manager and Cisco ThousandEyes, ensure you meet these prerequisites.

- Before deploying the Cisco ThousandEyes Enterprise agent, create an account on the Cisco ThousandEyes portal and obtain an account group token. The token authenticates the agent with Cisco ThousandEyes and associates it with the correct account.

For information on obtaining the account group token, see *Where Can I Get the Account Group Token?* on Cisco ThousandEyes Documentation portal.

- The Cisco ThousandEyes Enterprise agent requires DNS name resolution and HTTP/HTTPS connectivity to discover and register with the Cisco ThousandEyes portal. Ensure that this connectivity exists before deploying the agent by configuring the appropriate firewall rules, NAT settings, upstream routing, and other related settings.

For more information on the required firewall configuration, see *Firewall Configuration for Enterprise Agents* on Cisco ThousandEyes Documentation portal.

Restrictions for extending visibility with SD-WAN manager and Cisco ThousandEyes

Outlines limitations and configuration requirements when using Cisco ThousandEyes Enterprise agent with Cisco IOS XE Catalyst SD-WAN devices.

AppRoute data policies do not affect probes sourced from virtual Port-Group interfaces

Cisco ThousandEyes Enterprise agent probes are sourced from Virtual Port-Group interfaces and are not affected by AppRoute data policies.

Browser-based application tests not supported

The Cisco ThousandEyes Enterprise agent, hosted natively as a container application on Cisco IOS XE Catalyst SD-WAN devices, does not support browser-based application tests, such as page load test and transaction test.

Limitations of ThousandEyes instance modification

For every configuration change to the ThousandEyes instance, you must uninstall or deactivate and then reinstall and reactivate it for the changes to take effect.

- For Cisco IOS XE Catalyst SD-WAN devices prior to Cisco IOS XE Release 17.6.1, you can install the Docker Enterprise agent image either directly from ThousandEyes servers, or by uploading it using SCP, FTP, TFTP, or USB storage, depending on internet accessibility. It depends on whether the router has direct internet access or not.
- For Cisco IOS XE Catalyst SD-WAN devices after Cisco IOS XE Release 17.6.1, you can install the Enterprise Agent using bootflash, in addition to the previous methods.

Configure a Cisco ThousandEyes enterprise agent using a configuration group

Configure Cisco ThousandEyes Enterprise Agent settings using the ThousandEyes feature in a configuration group.

Configure Cisco ThousandEyes Enterprise Agent settings to enable network monitoring and performance testing capabilities within your SD-WAN fabric.

Use this procedure to configure Cisco ThousandEyes Enterprise Agent settings using the ThousandEyes feature in a configuration group. This allows you to deploy standardized ThousandEyes configurations across multiple devices in your network.

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Follow these steps to configure a Cisco ThousandEyes Enterprise Agent using a configuration group:

Procedure

1. From the SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.
2. Create and configure a ThousandEyes feature in Other profile.
   a. Configure ThousandEyes parameters.

   Table 70: Parameters

Parameter Scope	Scope Description
Device Specific (indicated by a host icon)	Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Cisco Catalyst SD-WAN device to a device template. When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Cisco Catalyst SD-WAN device to a device template. To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, host name, GPS location, and site ID.
Global (indicated by a globe icon)	Enter a value for the parameter and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.

   b. Configure the ThousandEyes settings.

Table 71: Settings

Field	Description
Type	Choose a feature from the drop-down list.
Feature Name	Enter a name for the feature.
Description	Enter a description of the feature. The description can contain any characters and spaces.
Account Group Token	Enter the Cisco ThousandEyes Account Group Token.
VPN	Service VPN. The **Global** or the **Device Specific** setting indicates service VPN. When you set the VPN configuration as a **Global** or a **Device Specific** setting, enter the ID of the service VPN in which you want to provision the Cisco ThousandEyes Enterprise agent.
Management IP	Enter an IP address for the Cisco ThousandEyes Enterprise agent. This field is available only when you specify the service VPN.
Management Subnet	Choose a subnet mask from the drop-down list for the Cisco ThousandEyes Enterprise agent. This field is available only when you specify the service VPN. **Note** This IP-prefix address (**Management IP** and **Management Subnet**) must be unique within the fabric and must not overlap with the IP addresses of other branch agents.
Agent Default Gateway	Enter a default gateway address. This IP address is assigned to the virtual port group of the router. This field is available only when you specify the service VPN.
Name Server IP	Enter the IP address of your preferred DNS server. This server can exist within or outside the Cisco Catalyst SD-WAN fabric but must be reachable from the service VPN.
Host Name	Enter the hostname that the agent must use when registering with the Cisco ThousandEyes portal. By default, the agent uses the hostname of the Cisco IOS XE Catalyst SD-WAN device.

Field	Description
Proxy Type	If the Cisco ThousandEyes Enterprise agent must use proxy server for external access, choose one of these as proxy type: • **static** • **PAC** • **none** Static proxy settings: • **Proxy Host**: Set the configuration as a **Global** setting and enter the hostname of the proxy server. • **Proxy Port**: Set the configuration as a **Global** setting and enter the port number of the proxy server. PAC settings: • **PAC URL**: Set the configuration as a **Global** setting and enter the URL of the proxy auto-configuration (PAC) file.

The ThousandEyes feature is configured in the configuration group and ready to be deployed to devices.

What to do next

Also see Deploy a configuration group.

Upload the Cisco ThousandEyes Enterprise Agent software to SD-WAN Manager

Configure the Cisco ThousandEyes Enterprise Agent software upload to make it available for installation through SD-WAN Manager.

Perform this task to make the Cisco ThousandEyes Enterprise Agent software available for installation through SD-WAN Manager.

This task enables you to upload and manage Cisco ThousandEyes Enterprise Agent software through the SD-WAN Manager interface for subsequent deployment to network devices.

Before you begin

Download the latest version of Cisco ThousandEyes Enterprise agent software from the Cisco ThousandEyes Agent Settings page.

Follow these steps to upload the Cisco ThousandEyes Enterprise Agent software to SD-WAN Manager:

Procedure

1. From the SD-WAN Manager menu, choose **Maintenance** > **Software Repository**.
2. Click **Virtual Images**.

3. Click **Upload Virtual Image** > **Manager**.
4. In the **Upload VNF's Package to Manager** dialog box, browse to select the downloaded Cisco ThousandEyes Enterprise Agent software file, or drag and drop the file into the dialog box.
5. Enter a description for the file.
6. (Optional) Add desired tags.
7. Click **Upload**.

The Cisco ThousandEyes Enterprise Agent software is now uploaded and available in the software repository for installation on devices.

What to do next

Proceed to install the uploaded Cisco ThousandEyes Enterprise agent software on relevant devices as needed.

Provision Cisco ThousandEyes Enterprise Agent in a Service VPN or Transport VPN (VPN0)

Configure Cisco ThousandEyes Enterprise agent in a service VPN to gain visibility into SD-WAN overlay and underlay network performance.

You can provision the Cisco ThousandEyes Enterprise agent in a service VPN for more visibility into the performance of the Cisco Catalyst SD-WAN overlay and underlay networks.

When you host the ThousandEyes agent on a router, you can deploy it in either a Service VPN or the Transport VPN (VPN0), based on your functional requirements and network topology. Deploying the ThousandEyes agent in VPN0 offers a simple routing approach when you need to send probe traffic over a single available underlay WAN link. In environments with multiple WAN links, Cisco recommends deploying the ThousandEyes agent in a Service VPN. This deployment method gives you granular control and enables you to create policies that direct probe traffic over specific underlay WAN paths, effectively simulating real-world traffic flows. If you deploy the ThousandEyes agent in VPN0 in a multi-WAN environment, the router load-balances probe traffic across all available WAN links, which may result in non-actionable monitoring insights.

Before you begin

- Ensure that DNS and NAT are correctly configured so that the Cisco ThousandEyes Enterprise Agent can access and connect to the Cisco ThousandEyes application.
- Upload Cisco ThousandEyes Enterprise agent software to SD-WAN Manager software repository.

  Note

  If multiple versions of the Cisco ThousandEyes Enterprise agent software are present in the SD-WAN Manager software repository, while provisioning the agent, SD-WAN Manager installs and activates the latest version of the agent software.

- For application monitoring use cases, deploy the ThousandEyes agent in the Service VPN and use an SD-WAN data policy to send ThousandEyes probes across transports

Procedure

1. Create feature template for the Cisco ThousandEyes Enterprise agent:
   a) From the Cisco SD-WAN Manager menu, choose **CONFIGURATION** > **Templates**.
   b) Click **Feature Templates**, and click **Add Template** to select an appropriate device model.

> **Note**
>
> In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled as **Feature**.

   c) Choose the supported devices to which you want to apply this template.
   d) In the **Other Templates** section, click **ThousandEyes Agent**.
   e) **Template Name**: Enter a name for the template. Ensure that the template name is unique.
   f) **Description**: Enter a description for the template.
   g) In the **BASIC CONFIGURATION** section, configure these fields:

Account Group Token	Enter the Cisco ThousandEyes Account Group Token.
VPN	1. Set the VPN CONFIGURATION as a **Global** or a **Device Specific** setting. 2. Enter the ID of the service VPN in which you want to provision the Cisco ThousandEyes Enterprise agent.
Agent IP Address	Enter an IP address for the Cisco ThousandEyes Enterprise agent. This IP Address should be unique within the fabric and should not overlap with the IP addresses of other branch agents.
Agent Default Gateway	Enter a default gateway address. This IP address is assigned to the virtual port group of the router.

> **Note**
>
> You can create and allocate a service subnet for the agent network. Two usable IP addresses are required to provision the Cisco ThousandEyes Enterprise agent on each Cisco IOS XE Catalyst SD-WAN device. One of the IP addresses must be assigned to the agent and second IP address to the router virtual port group.

   h) In the **ADVANCED** section, configure these fields:

Name Server	(Optional parameter from Cisco vManage Release 20.7.1 and Cisco IOS XE Release 17.7.1a) Enter the IP address of your preferred DNS server. This server can exist within or outside the Cisco Catalyst SD-WAN fabric but must be reachable from the service VPN.
Hostname	(Optional) Enter the hostname that the agent must use when registering with the Cisco ThousandEyes portal. By default, the agent uses the Cisco IOS XE Catalyst SD-WAN device's hostname.

Web Proxy Type	(Optional) If the Cisco ThousandEyes Enterprise agent must use proxy server for external access, choose one of these as proxy type: • **Static** • **PAC** Static proxy settings: • **Proxy Host**: Set the CONFIGURATION as a **Global** setting and enter the hostname of the proxy server. • **Proxy Port**: Set the CONFIGURATION as a **Global** setting and enter the port number of the proxy server. PAC settings: • **PAC URL**: Set the CONFIGURATION as a **Global** setting and enter the URL of the proxy auto-CONFIGURATION (PAC) file.

i) Click **Save**.

2. Attach the ThousandEyes Agent feature template to device template:
   a) From the Cisco SD-WAN Manager menu, choose **CONFIGURATION** > **Templates**.
   b) Click **Device Templates**.

> **Note**
>
> In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled as **Device**

   c) Find the device template for the target device.
   d) For this template, click **...**, and click **Edit**.
   e) Click **Additional Templates**.
   f) Click **Update**.
   g) Update necessary variables, if any, and click **Next**.
   h) Review the CONFIGURATION and click **Configure Devices**.
3. Repeat Step 2 for each device on which you want to deploy the Cisco ThousandEyes Enterprise agent.

The Cisco ThousandEyes Enterprise agent is deployed on the chosen devices. The agent registers with and establishes secure communication with the cloud-based Cisco ThousandEyes application to receive necessary updates and CONFIGURATION.

What to do next

You can configure various tests and see resultant network and application telemetry data on the Cisco ThousandEyes portal.

Provision a Cisco ThousandEyes enterprise agent in a service VPN using CLI

Configure a Cisco ThousandEyes Enterprise agent in a service VPN using CLI commands to enable network monitoring and testing capabilities.

This task enables you to provision the Cisco ThousandEyes Enterprise agent on Cisco IOS XE Catalyst SD-WAN devices to provide network monitoring and testing capabilities within a service VPN environment.

Use the example command sequences described in this section to provision the Cisco ThousandEyes Enterprise agent on Cisco IOS XE Catalyst SD-WAN devices through a device CLI template or an add-on CLI template.

Follow these steps to provision a Cisco ThousandEyes Enterprise agent in a service VPN using CLI:

Before you begin

- Ensure that the appropriate DNS and NAT configuration exists to enable the Cisco ThousandEyes Enterprise agent to discover and connect to the Cisco ThousandEyes application.
- Upload Cisco ThousandEyes Enterprise agent software to SD-WAN Manager.

> **Note**
>
> If you have uploaded more than one version of the Cisco ThousandEyes Enterprise agent software to the SD-WAN Manager software repository, while provisioning the agent, SD-WAN Manager installs and activates the latest version of the agent software.

Procedure

1. Enable IOX on the device.

   Example

   ```
   iox
   ```

2. Configure virtual port group. The virtual port group acts as the gateway for the Cisco ThousandEyes Enterprise agent.

   Example

   ```
   interface VirtualPortGroup4
    vrf forwarding 100
     ip address 192.168.61.1 255.255.255.252
   ```

3. Configure app-hosting paramters for the Cisco ThousandEyes Enterprise agent.

   Example

   ```
   app-hosting appid te
   app-vnic gateway0 virtualportgroup 4 guest-interface 0
    guest-ipaddress 192.168.61.2 netmask 255.255.255.252
   app-default-gateway 192.168.61.1 guest-interface 0
   app-resource docker
    prepend-pkg-opts
    run-opts 1 "-e TEAGENT_ACCOUNT_TOKEN=z0kemf"
    run-opts 2 "--hostname ISR4461TE"
    run-opts 3 "-e TEAGENT_PROXY_TYPE=STATIC -e
   TEAGENT_PROXY_LOCATION=proxy-exmaple.com:80"
   name-server0  192.168.168.183
   start
   ```

Note

- Use the proxy configuration only if the Cisco ThousandEyes agent does not have an Internet access without a proxy. The hostname is optional. If you do not provide the hostname during the installation, the device hostname is used as the Cisco ThousandEyes agent hostname, which appears on the Cisco ThousandEyes portal. From Cisco IOS XE Release 17.7.1a, the DNS name server information is optional.
- If the Cisco ThousandEyes agent uses a private IP address, establish a connection to the device through NAT.

The Cisco ThousandEyes Enterprise agent is successfully provisioned and running in the service VPN. The agent can now perform network monitoring and testing functions and communicate with the Cisco ThousandEyes application.

Uninstall the Cisco ThousandEyes enterprise agent software

Configure a device template to remove the Cisco ThousandEyes Enterprise Agent software from devices by setting the ThousandEyes Agent template to None.

Remove the Cisco ThousandEyes Enterprise Agent software from a device by updating its configuration template so the software is no longer provisioned or managed through SD-WAN Manager.

Use this procedure when you need to stop managing ThousandEyes agent software on specific devices while maintaining their existing device template configuration.

Procedure

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

   Note

   In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled as **Device**

3. Find the device template for the device from which the Cisco ThousandEyes agent software must be removed.
4. For this template, click **...** and then click **Edit**.
5. Click **Additional Templates**.
6. In the **Additional Templates** section, for **ThousandEyes Agent** choose **None** from the drop-down list.
7. Click **Update**.
8. Update necessary variables, if any, and click **Next**.
9. Review the configuration and click **Configure Devices**.

The Cisco ThousandEyes Enterprise Agent software is removed from the selected devices and is no longer provisioned or managed through the device template.

What to do next

Verify that the agent software has been removed from the affected device(s) by checking device status and software inventory.

Upgrade the Cisco ThousandEyes enterprise agent software

Configure Cisco ThousandEyes Enterprise Agent software upgrades on edge routers through SD-WAN Manager to ensure agents have the latest enhancements and security updates.

Upgrade Cisco ThousandEyes Enterprise Agent software on edge routers through SD-WAN Manager.

This section provides procedure to upgrade the Cisco ThousandEyes Enterprise Agents have the latest enhancements and security updates.

Before you begin

Download a new version of Cisco ThousandEyes Enterprise agent software and upload the software to SD-WAN Manager. See *Upload Cisco ThousandEyes Enterprise Agent Software to Cisco SD-WAN Manager*.

Procedure

1. From the SD-WAN Manager menu, choose **Maintenance** > **Software Upgrade**.
2. Select the Cisco IOS XE Catalyst SD-WAN devices on which you want to upgrade the Cisco ThousandEyes Enterprise agent software.
3. Click **Upgrade Virtual Image**.
4. In the **Virtual Image Upgrade** dialog box, choose the new version of the Cisco ThousandEyes Enterprise agent software from the drop-down list.
5. Click **Upgrade**.
6. On the **Maintenance** > **Software Upgrade** page, select the Cisco IOS XE Catalyst SD-WAN devices on which you upgraded the Cisco ThousandEyes Enterprise agent software.
7. Click **Activate Virtual Image**.

The Cisco ThousandEyes Enterprise Agent software is upgraded on the selected edge routers.

What to do next

Verify agent status and functionality on each router.

Troubleshoot the Cisco ThousandEyes Enterprise Agent on Cisco IOS XE Catalyst SD-WAN devices

Configure troubleshooting procedures to identify and resolve issues with the Cisco ThousandEyes Enterprise Agent running on supported devices.

Identify and resolve issues with the Cisco ThousandEyes Enterprise Agent running on supported Cisco IOS XE Catalyst SD-WAN devices.

Use this troubleshooting procedure when the Cisco ThousandEyes Enterprise Agent is not functioning correctly on your device and you need to diagnose configuration or operational issues.

Procedure

1. Connect to Cisco ThousandEyes Enterprise agent.

```
Device#app-hosting connect appid Appid session /bin/bash
```

2. To verify the agent configuration, check the following CFG file: `/etc/te-agent.CFG`.
3. To view the agent logs, check the following file: `/var/log/agent/te-agent.log`.

After completing these steps, you will have access to the agent configuration and log files necessary to diagnose and resolve ThousandEyes Enterprise Agent issues.