Lawful intercept 2.0

Feature history for lawful intercept 2.0

In Lawful Intercept 2.0, controllers provide the intercept key information to the LEA.

Table 1: Feature History

Feature Name	Release Information	Description
Lawful Intercept 2.0	Cisco vManage Release 20.9.1	This feature introduces Lawful Intercept Version 2.0. In the Lawful Intercept 2.0 feature, key information is provided to a law enforcement agency (LEA) by the Cisco Catalyst SD-WAN routers and Control Components so that they can decrypt the Cisco Catalyst SD-WAN IPsec traffic captured by the Managed Service Provider (MSP). This helps the LEA decrypt the encrypted network traffic information. For information on Lawful Intercept 1.0, see the chapter Lawful Intercept in the Cisco Catalyst SD-WAN Policies Configuration Guide.

Feature Name	Release Information	Description

Lawful Intercept 2.0 Enhancements	Cisco vManage Release 20.10.1	This feature enhances the Cisco SD-WAN Manager GUI and the troubleshooting options available for the Lawful Intercept feature in Cisco Catalyst SD-WAN.
		• Cisco SD-WAN Manager GUI enhancements:
		  • A **Sync to vSmart** button to synchronize a newly created intercept configuration with the Cisco SD-WAN Controller.
		  • A toggle button to enable or disable an intercept.
		  • A progress page to display the status of synchronization and activation.
		  • A red dot on the task list icon in the Cisco SD-WAN Manager toolbar to indicate any new lawful intercept tasks.
		  • A task list pane to view a list of active and completed lawful intercept tasks.
		  • An intercept retrieve option **Get IRI** to retrieve key information or Intercept Related Information (IRI) from the Cisco SD-WAN Controller.
		• Ability to troubleshoot Cisco SD-WAN Controller and Cisco SD-WAN Manager using the debug logs and admin tech files.

Lawful Intercept 2.0 Enhancements	Cisco Catalyst SD-WAN Manager Release 20.12.1	This feature extends Lawful Intercept to multitenancy mode, and provides support for Cisco SD-WAN Manager clusters. For more information on Cisco SD-WAN Manager clusters, see Cluster Management.

Lawful intercept 2.0

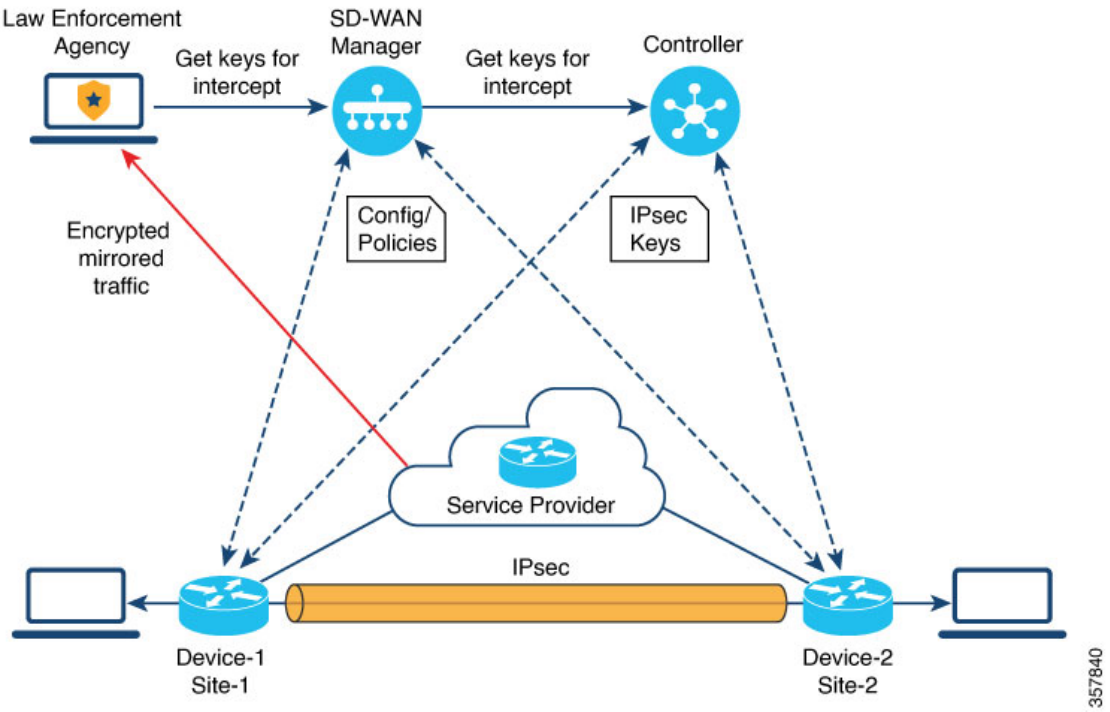
Lawful intercept 2.0 is a traffic mirroring feature that

- allows an LEA to get a copy of network traffic for analysis or evidence
- implements traffic mirroring outside the scope of Cisco Catalyst SD-WAN, and
- provides key information through Cisco SD-WAN Manager and Cisco SD-WAN Controller to decrypt captured encrypted traffic.

Architecture characteristics

From Cisco vManage Release 20.9.1, Cisco Catalyst SD-WAN implements a new architecture for Lawful Intercept.

Figure 1: Lawful Intercept 2.0 Architecture



The new architecture has the following characteristics:

- Traffic mirroring is outside the scope of Cisco Catalyst SD-WAN. The LEA works with the corresponding service provider to capture network traffic for mirroring.

Note In the illustration above, the service provider is an underlay connection and the IPsec tunnel is an overlay connection.

- Because the captured network traffic is encrypted, Cisco SD-WAN Manager and Cisco SD-WAN Controller provide key information to the LEA.
- The LEA retrieves the keys from Cisco SD-WAN Manager to decrypt Cisco Catalyst SD-WAN IPsec traffic. The LEA ensures that they retrieve key information is retrieved during each rekey period. The rekey period is provided by the service provider. For more information about retrieving keys, see Retrieving an intercept, on page 8. For information on rekey period, see Configure Data Plane Security Parameters.

A Lawful Intercept administrator is solely responsible for configuring intercepts and creating Lawful Intercept API users who perform Lawful Intercepts. A Cisco SD-WAN Manager administrator can create an account for the Lawful Intercept administrator; the administrator must be a member of the **li-admin** group. For more information about creating an account for a Lawful Intercept administrator, see Create Lawful Intercept Administrator.

Prerequisites for lawful intercept 2.0

- A Cisco SD-WAN Controller must be set to **Manager mode**.
- For more information about decrypting the IPsec traffic in Cisco Catalyst SD-WAN, contact Cisco Support or Cisco Sales team.

Benefits of lawful intercept 2.0

Benefits of lawful intercept 2.0 are operational advantages that

- eliminate the need to configure edge devices for lawful intercepts
- enable service providers to capture data traffic for interception without intercepting traffic directly from edge devices, and
- streamline the interception process through centralized key management.

Key operational improvements

Lawful intercept 2.0 provides the following operational improvements:

- It is not necessary to configure edge devices for Lawful Intercepts.

Note To configure an intercept, an administrator must select the edge devices that have to be included in the intercept. This is necessary because the key information that is retrieved from Cisco SD-WAN Manager also includes the keys for the selected devices.

- The service provider captures the data traffic for interception. Traffic is not intercepted from the edge devices.

Configuring lawful intercept 2.0 workflow

Note The Lawful Intercept feature can be configured only through Cisco SD-WAN Manager, and not through the CLI.

Summary

The key components involved in the lawful intercept 2.0 configuration workflow are:

- Lawful Intercept Administrator: Manages the overall lawful intercept configuration and oversight
- Lawful Intercept API User: Provides programmatic access to intercept functionality

- Intercept Configuration: Defines the specific parameters and targets for traffic monitoring
- Cisco SD-WAN Manager: Serves as the centralized management platform for configuration

Workflow

These are the stages of configuring lawful intercept 2.0 workflow:

1. Create the Lawful Intercept Administrator to establish administrative oversight for intercept operations.

   Create Lawful Intercept Administrator

2. Create the Lawful Intercept API User to enable programmatic access to intercept functionality.

   Create Lawful Intercept API User

3. Create the intercept configuration to define the specific parameters for traffic monitoring.

   Create an Intercept

Create a lawful intercept administrator

This task creates a dedicated administrator account for managing lawful intercept operations, providing the necessary user access and permissions for legal compliance activities.

A lawful intercept administrator account is required to manage lawful intercept operations within the system. This specialized administrator role has specific permissions and access rights needed for legal compliance activities.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Lawful Intercept**.

Step 2 Click **Add User** to create a Lawful Intercept administrator user account.

Step 3 In the **Full Name** field, enter a full name for the Lawful Intercept administrator.

Step 4 In the **User Name** field, enter a user name for the Lawful Intercept administrator.

The user name must be prefixed with **li-**.

Step 5 In the **Password** field, enter a password for the Lawful Intercept administrator.

Step 6 Confirm the password in the **Confirm Password** field.

Step 7 From the **User Group** drop-down list, choose **li-admin**, and then click **Add**.

The newly created Lawful Intercept administrator user account is displayed in the **Users** window.

A Lawful Intercept administrator account has been successfully created with the appropriate user group permissions and is ready for use in managing lawful intercept operations.

Create a lawful intercept API user

This task creates a Lawful Intercept API User account for Law Enforcement Agency users who log in and retrieve key information using Cisco SD-WAN Manager's REST API. These are the users who perform a lawful intercept of the Cisco Catalyst SD-WAN IPsec traffic.

The LEA use **`https://{vmanage_ip}/dataservice/li/intercept/retrieve/<intercept_id>`** to retrieve the key information.

Procedure

Step 1 Log in to Cisco SD-WAN Manager as a Lawful Intercept administrator.

Note
When a Lawful Intercept administrator logs in to Cisco SD-WAN Manager, only the **Monitor** and **Administration** options are available in the Cisco SD-WAN Manager menu.

Step 2 From Cisco SD-WAN Manager menu, choose **Administration** > **Lawful Intercept**.

Step 3 Click **Add User** to create an Lawful Intercept API user account.

Step 4 In the **Full Name** field, enter a full name for the Lawful Intercept API user.

Step 5 In the **User Name** field, enter a user name for the Lawful Intercept API user. The user name must be prefixed with **li-**.

Step 6 In the **Password** field, enter a password for the Lawful Intercept API user.

Step 7 Confirm the password in the **Confirm Password** field.

Step 8 From the **User Group** drop-down list, choose **li-API**, and click **Add**.

The Lawful Intercept API user account is created and displayed in the **Users** window. The LEA can now log in to Cisco SD-WAN Manager using this account to retrieve key information.

Create an intercept

Create an intercept to enable the collection of intercept data as part of lawful intercept operations on your Cisco Catalyst SD-WAN network.

Minimum supported release: Cisco vManage Release 20.9.1 and Cisco Catalyst SD-WAN Control Components Release 20.9.1.

When an edge device is added for interception, all its peer devices, which are connected in the same network, are also available for Lawful Interception.

Before you begin

You must specify an intercept warrant for all the edge devices that are added to the intercept.

Follow these steps to create an intercept:

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Lawful Intercept**.

Step 2 Click the **Intercepts** tab, and then click **Add Intercepts**.

Step 3 Cisco Catalyst SD-WAN Manager Release 20.12.1 and later releases: From the **Tenant** drop-down list, choose a tenant.

For more information about adding a tenant, see Add a New Tenant.

Step 4 In the **Intercept ID** field, enter a number.

Enter a minimum of two digits and a maximum of 25 digits.

Step 5 In the **Description** field, enter a description for the intercept.

Step 6 By default the **Enable** toggle button is enabled.

However, the intercept remains in an inactive state after it is created.

Step 7 Click **Next**.

In single-tenant mode, the **Add Edge Devices** pop-up window displays all the edge devices in the Cisco Catalyst SD-WAN network.

Cisco Catalyst SD-WAN Manager Release 20.12.1 and later releases:

In multi-tenant mode, the **Add Edge Devices** pop-up window displays all the single-tenant edge devices associated with the selected tenant.

Step 8 Click one or more edge device names to add to the intercept and click **Next**.

Cisco SD-WAN Manager provides the keys for the edge devices selected here.

Note
Specify an intercept warrant for all the edge devices that are added to the intercept.

Step 9 The **Add LI API users** pages displays all the LI-API users created by the Lawful Intercept administrator.

Step 10 Click one or more user names to add to the intercept.

The users selected here can retrieve key information that is required for interception from Cisco SD-WAN Manager. For information on how keys are retrieved for an intercept, see Retrieve an Intercept.

Step 11 Click **Summary**.

The summary of the intercept is displayed.

Step 12 Click **Submit**.

The **Intercepts** page displays the configured intercept.

Step 13 Click **Sync to vSmart** to synchronize the configured intercept configuration in Cisco SD-WAN Manager with Cisco SD-WAN Controller.

A progress page displays the status of the synchronization and activation. After successful synchronization, the **Activate State** field displays a green check mark.

Note
The **Activate State** field displays a green check mark status only if Cisco SD-WAN Controller is set to **Manager** mode.

If there are any additional Lawful Intercept tasks, a red dot is displayed on the task list icon in the Cisco SD-WAN Manager toolbar. Click the tasks list icon to view a list of all the active and completed Lawful Intercept tasks. You can view up to 500 latest Lawful Intercept tasks.

If an intercept is modified, the **Sync to vSmart** button is enabled. Click **Sync to vSmart** to synchronize the intercept configuration in Cisco SD-WAN Manager with Cisco SD-WAN Controller.

Note
The **Sync to vSmart** button is enabled only when a new intercept is created, or when an intercept is edited or deleted.

To retrieve key information that is required for interception, click **…**, and then click **Get IRI**. The IRI is retrieved from Cisco SD-WAN Controller and displayed in Cisco SD-WAN Manager.

Retrieving an intercept

An LEA is responsible to periodically retrieve key information because this information is required to decrypt the traffic captured by the MSP.

Summary

The key components involved in the intercept retrieval process are:

- LEA: Initiates the key information retrieval request as a Lawful Intercept API user
- Cisco SD-WAN Manager: Receives and forwards the retrieval request to the appropriate Cisco SD-WAN Controller
- Cisco SD-WAN Controller: Retrieves the key information for the specified intercept ID and returns it in JSON format

Workflow

The intercept retrieval process involves the following stages:

1. An LEA logs in to Cisco SD-WAN Manager as a Lawful Intercept API user.
2. After a Lawful Intercept API user is authenticated, the LEA sends a request using the Cisco SD-WAN Manager REST APIs specifying the intercept ID that it wants to get the key information for.

   An LEA can retrieve key information by using Cisco Catalyst SD-WAN Manager REST APIs.
3. When a request from the LEA is received by Cisco SD-WAN Manager, Cisco SD-WAN Manager forwards the request to the Cisco SD-WAN Controller on which intercepts are configured.
4. Cisco SD-WAN Controller then retrieves the key information for the specified intercept ID and returns the key information to Cisco SD-WAN Manager in JSON format.

Troubleshoot Cisco SD-WAN Controller for lawful intercept from Cisco SD-WAN Manager

This task helps you troubleshoot any issues in Cisco SD-WAN Controller and Cisco SD-WAN Manager for lawful intercept using available diagnostic tools.

Minimum supported release: Cisco vManage Release 20.10.1and Cisco Catalyst SD-WAN Control Components Release 20.10.1

Cisco SD-WAN Manager offers debug logs and admin tech files to troubleshoot any issues in Cisco SD-WAN Controller and Cisco SD-WAN Manager.

Procedure

Step 1 View debug logs to troubleshoot Cisco SD-WAN Controller from Cisco SD-WAN Manager.

a. From Cisco SD-WAN Manager menu, choose **Administration** > **Lawful Intercept**.

b. Click the **Devices** tab.

c. Click **...** adjacent to the device that you want to view the debug logs, and choose **Debug Log**.

d. In the **Log Files** drop-down list, choose the name of the log file.

The lower part of the window displays the log information.

Step 2 Use debug logs and admin tech files to troubleshoot Cisco SD-WAN Manager and Cisco SD-WAN Controller from Cisco SD-WAN Manager.

For more information about generating an admin tech file, see Generate Admin-Tech Files.

Note
Note: When an li-admin user generates an admin-tech file using Cisco SD-WAN Manager, it will only include the 'local0.log' file. Other log files that pertain to system diagnostic information are not included.

You can now troubleshoot Cisco SD-WAN Controller and Cisco SD-WAN Manager issues using the debug logs and admin tech files accessed through the lawful intercept interface.