Lawful intercept

Feature history for lawful intercept

The Lawful Intercept feature supports service providers in meeting the requirements of law enforcement agencies (LEA) to provide electronic surveillance as authorized by a judicial or administrative order. The surveillance is performed using wiretaps to intercept Voice-over-Internet protocol (VoIP) or data traffic going through the edge routers. The LEA delivers a request for a wiretap to the target's service provider, who is responsible for intercepting data communication to and from the individual using IP sessions. A user session is tapped using either the Source and Destination IP addresses, or VRF name, which is translated to a vrf-tableid value within the router.

Table 1: Feature History

Feature Name	Release Information	Description
Encryption of Lawful Intercept Messages	Cisco IOS XE Catalyst SD-WAN Release 16.12.1b	This feature encrypts lawful intercept messages between a Cisco IOS XE Catalyst SD-WAN device and a media device using static tunnel information.

Lawful intercept

Lawful intercept is a process that enables a Law Enforcement Agency (LEA) to perform electronic surveillance on an individual (a target) as authorized by a judicial or administrative order. To facilitate the lawful intercept process, certain legislation and regulations require service providers (SPs) and Internet service providers (ISPs) to implement their networks to explicitly support authorized electronic surveillance.

Lawful intercept process

When triggering a lawful intercept for communications from Site A to Site B, the edge platform duplicates the traffic and sends an unencrypted copy of the traffic to a target server, which hosted in the customer network designed for Lawful Intercept. Cisco SD-WAN Manager ensures that Cisco SD-WAN Manager users (non-Lawful Intercept users), who have access to Site A and Site B for any information, are unaware of the duplicated flow of information.

Figure 1: Cisco Catalyst SD-WAN Lawful Intercept Workflow

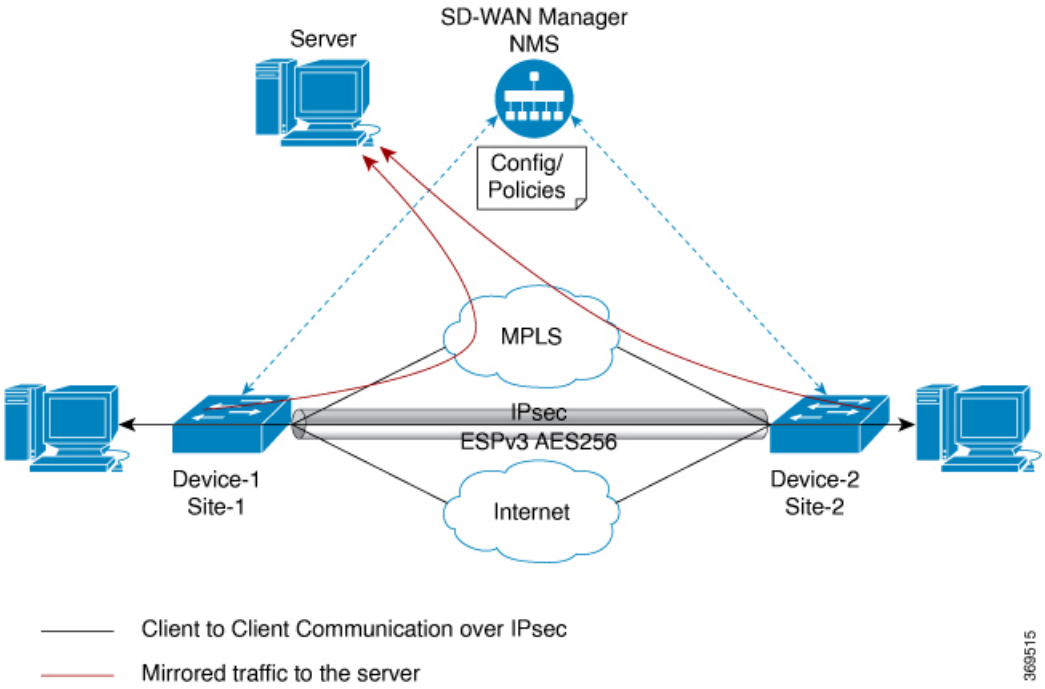
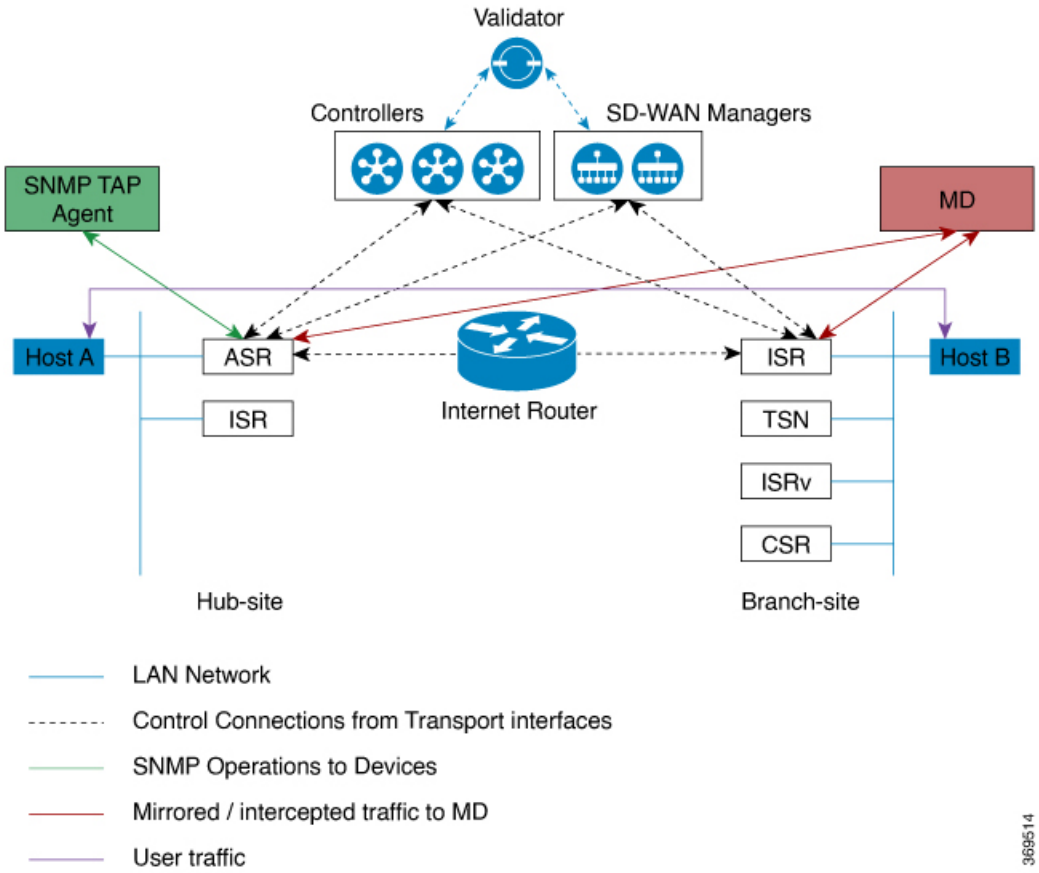


Figure 2: Cisco Catalyst SD-WAN Lawful Intercept Process



Licence-based lawful intercept

Cisco Catalyst SD-WAN solution is a term-based licensed feature. This feature license enables the Cisco SD-WAN Manager component of the Cisco Catalyst SD-WAN solution and allows the customer to access the Lawful Intercept function. Once the Lawful Intercept license is enabled on the solution, Cisco SD-WAN Manager provides a new privilege in the Manage Users menu of the Cisco SD-WAN Manager UI. By default, this privilege is available to all admin users. In addition, administrators can assign the Lawful Intercept privilege to any other user.

Any user with Lawful Intercept privilege would be able to enable Lawful Intercept function on an edge device in the WAN network. All changes made by any user with Lawful Intercept function would be audit logged and changes will be recorded just like any other change made by any user in the system.

After acquiring a court order or warrant to perform surveillance, any user with Lawful Intercept privilege will be able to make Lawful Intercept related changes on sites with a warrant.

1. Install license for Lawful Intercept on Cisco SD-WAN Manager.
2. Create an lawful intercept admin (liadmin) user on Cisco SD-WAN Manager. The **liadmin** user must be associated with the user group, Basic.
3. Login to Cisco SD-WAN Manager as **liadmin** user and configure Lawful Intercept specific templates.

4. Cisco SD-WAN Manager automatically pushes templates to all Cisco IOS XE Catalyst SD-WAN devices with Lawful Intercept compatible images.
5. Configuration is pushed to device from Cisco SD-WAN Manager using the following:
   a. SNMP TAP MIB configuration
   b. SNMP Access list (li-acl keyword)
   c. MD List
6. SNMP SET is sent to device to achieve the following goals:
   a. To setup and activate MD entry on Cisco IOS XE Catalyst SD-WAN devices.
   b. To setup and activate stream to be intercepted.
   c. To activate or deactivate intercept
7. Mediation Device receives the intercepted or mirrored traffic.

VRF-aware lawful intercept

VRF Aware Lawful Intercept is the ability to provision a Lawful Intercept wiretap on IPv4 data in a particular VPN. This feature allows a LEA to lawfully intercept targeted data within that VPN. Only IPv4 data within that VPN is subject to the VRF-based Lawful Intercept tap.

To provision a VPN-based IPv4 tap, the LI administrative function (running on the mediation device) uses the CISCO-IP-TAP-MIB to identify the name of the VRF table that the targeted VPN uses. The VRF name is used to select the VPN interfaces on which to enable LI in order to execute the tap. The device determines which traffic to intercept and which mediation device to send the intercepted packets based on the VRF name (along with the source and destination address, source and destination port, and protocol).

Prerequisites for lawful intercept

Access to the Cisco Lawful Intercept MIB view should be restricted to the mediation device and to system administrators who need to be aware of lawful intercepts on the router. To access the MIB, users must have level-15 access rights on the router.

For the router to communicate with the mediation device to execute a lawful intercept, the following configuration requirements must be met:

- The domain name for both the router and the mediation device must be registered in the Domain Name System (DNS). In DNS, the router IP address is typically the address of the FastEthernet0/0/0 interface on the router.
- The mediation device must have an access function (AF) and an access function provisioning interface (AFPI).
- You must add the mediation device to the Simple Network Management Protocol (SNMP) user group that has access to the CISCO-TAP2-MIB view. Specify the username of the mediation device as the user to add to the group.

- When you add the mediation device as a CISCO-TAP2-MIB user, you can include the mediation device's authorization password if you want. The password must be at least eight characters in length.

- You must configure SNMP service in Cisco SD-WAN Manager using the VPN Interface Ethernet page of Feature Template. See VPN Interface Ethernet section in Templates topic.

Install lawful intercept using Cisco Catalyst SD-WAN Manager

Note The following process must be repeated for every Cisco SD-WAN Manager node.

1. Connect to a Cisco SD-WAN Manager device as administrator
2. Request tools license

```
vm12# tools license request
Your org-name is: XYZ Inc
Your license-request challenge is:
Uwk3u4Vwkl8n632fKDIpKDEFkzfeJlhFQPOHopbvewmed0U83LQDgajO7GnmCIgA
```

3. Contact Cisco Support to generate the license using the output of Step 2.
4. Run the install file command and reboot:

```
vm12# tools license install file license.lic
License installed. Please reboot to activate.
vm12# reboot
Are you sure you want to reboot? [yes,no] yes

Broadcast message from root@vm12 (somewhere) (Tue Jan 22 17:07:47 2019):
Tue Jan 22 17:07:47 UTC 2019: The system is going down for reboot NOW!
Connection to 10.0.1.32 closed.
tester@vip-vmanage-dev-109:~$
```

5. Verify if the Lawful Intercept license is installed successfully, using the following command:

```
vm12# show system status
LI License Enabled  True
```

6. Create lawful intercept admin user using Cisco SD-WAN Manager.
7. Login to Cisco SD-WAN Manager using the lawful intercept admin credentials.

Note Use the **tools license remove-all** command to remove all licenses after reboot. You will not be able to re-install the previous license.

Lawful intercept MIBs

Due to its sensitive nature, the Cisco Lawful Intercept MIBs are only available in software images that support the Lawful Intercept feature.

These MIBs are not accessible through the Network Management Software MIBs Support page.

Restricting access to the lawful intercept MIBs

Only the mediation device and users who need to know about lawful intercepts must be allowed to access the Lawful Intercept MIBs. To restrict access to these MIBs, you must perform the following actions:

1. Create a view that includes the Cisco Lawful Intercept MIBs.
2. Create an SNMP user group that has read-and-write access to the view. Only users assigned to this user group can access information in the MIBs.
3. Add users to the Cisco LI user groups to define who can access the MIBs and any information related to lawful intercepts. Be sure to add the mediation device as a user in this group; otherwise, the router cannot perform lawful intercepts.

Note Detail MD5 authentication key generation algorithm is defined at https://tools.ietf.org/html/rfc3414#appendix-A.2.1

Restrict access to trusted hosts without encryption

SNMPv3 provides support for both security models and security levels. A security model is an authentication strategy that is set up for a user and the group in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level will determine the security mechanism employed when handling an SNMP packet.

Additionally, the SNMP support for the Named Access Lists feature adds support for standard named access control lists (ACLs) to several SNMP commands.

To configure a new SNMP group or a table that maps SNMP users to SNMP views, use the **snmp-server** command in global configuration mode.

In the following example, the access list named 99 allows SNMP traffic only from 10.1.1.1 to access Cisco IOS XE Catalyst SD-WAN devices. This access list is then applied to the SNMP user, testuser.

```
access-list 99 permit ip host 10.1.1.1
snmp-server user testuser INTERCEPT_GROUP v3 encrypted auth sha
testPassword1 priv aes testPassword2 access 99
```

SNMP traffic is only allowed from WAN interface (gigabitEthernet 1).

```
control-plane host
management-interface gigabitEthernet 1 allow snmp
```

Restrict trusted mediation device

In the following example, the **md-list** command allows an SNMP request **config MD** in the subnet 10.3.3.0/24.

When a Cisco IOS XE Catalyst SD-WAN device receives an SNMP request to create a mediation device, it first checks the Mediation Device List configuration information.

If the IP address of the mediation device is not in the configured Mediation Device List, the Mediation Device entry is not active.

```
md-list 10.3.3.0 255.255.255.0
```

Note You can configure up to a maximum of eight Mediation Device List subnets.

Configure lawful intercept

The following are the two components for Lawful Intercept Cisco SD-WAN Manager configuration:

- Lawful Intercept SNMP template – This template provisions the configuration for the following:
  - SNMPv3 group for lawful intercept – The group name is INTERCEPT_GROUP by default.
  - SNMPv3 users for lawful intercept – All users are restricted by an access list by default.
  - SNMPv3 view is configured by default. The view included Cisco TAP MIBs.
  - The following TAP MIBs are configured:
    - ciscoIpTapMIB
    - ciscoTap2MIB
    - ifIndex
    - ifDescr
- Lawful intercept access list template – The access list template provides configuration for the following:
  - Mediation Device-List configuration – Provides option to configure up to 8 subnets.
  - SNMP access-list – provides option to configure up to 8 subnets or host addresses, and a wildcard mask.

Configure lawful intercept using CLI

```
control-plane host
management-interface GigabitEthernet0/0/0 allow ftp ssh snmp
management-interface GigabitEthernet0/0/1 allow ftp ssh snmp
!
```

```
!
md-list 10.101.0.0 255.255.255.0
md-list 10.102.0.10 255.255.255.255
md-list 10.103.0.0 255.255.255.0
md-list 10.104.0.4 255.255.255.255
md-list 10.105.0.0 255.255.255.0
md-list 10.106.0.0 255.255.255.0
md-list 10.107.0.7 255.255.255.255
md-list 10.108.0.0 255.255.0.0
!
ip access-list standard li-acl
 permit 174.16.50.254
```

Example: Enabling mediation device access lawful intercept MIBs

The following example shows how to enable the mediation device to access the lawful intercept MIBs. It creates an SNMP view (tapV) that includes four LI MIBs (CISCO-TAP2-MIB, CISCO-IP-TAP-MIB, CISCO-802-TAP-MIB, and CISCO-USER-CONNECTION-TAP-MIB). It also creates a user group that has read, write, and notify access to MIBs in the tapV view.

```
snmp-server enable trap
snmp-server engineID local 766D616E6167652Dac10ff31
snmp-server group INTERCEPT_GROUP v3 noauth read INTERCEPT_VIEW write INTERCEPT_VIEW notify
 SNG_VIEW
snmp-server user UItestuser1 INTERCEPT_GROUP v3 encrypted auth md5
DA:B2:36:03:6A:5C:D0:6D:F6:D8:9C:5E:56:77:AD:43 priv aes 128
DA:B2:36:03:6A:5C:D0:6D:F6:D8:9C:5E:56:77:AD:43 access li-acl
snmp-server user UItestuser2 INTERCEPT_GROUP v3 encrypted auth md5
D2:01:1E:47:D8:9E:3E:B5:58:CD:90:0F:49:FC:36:56 priv aes 128
CF:32:C4:3E:34:27:3F:4A:D8:18:A7:19:E5:04:A7:DF access li-acl
!
snmp-server engineID local 766D616E6167652DAC10FF31
snmp-server group INTERCEPT_GROUP v3 noauth read INTERCEPT_VIEW write INTERCEPT_VIEW notify
 SNG_VIEW
snmp-server view INTERCEPT_VIEW ciscoIpTapMIB included
snmp-server view INTERCEPT_VIEW ciscoTap2MIB included
snmp-server view INTERCEPT_VIEW ifIndex included
snmp-server view INTERCEPT_VIEW ifDescr included
```

Encrypt lawful intercept traffic

Encryption of intercepted traffic between the router (the content Intercept Access Point (IAP)) and the Mediation Device (MD) is recommended.

The following is the required configuration:

- Configuring encryption in the router, and either an encryption client in the MD or a router associated with the MD to decrypt the traffic.
- Restricting access to trusted hosts.
- Configuring the VPN client.

Configure encryption in the device

To configure encryption, configure Authentication, Authorization, and Accounting (AAA) parameters. The following example shows how to configure the parameters:

```
aaa authentication login userauthen local
username <username> password 0 <password
```

In CISCO-TAP2-MIB, the source interface must be the tunnel interface of the Cisco IOS XE Catalyst SD-WAN devices and the destination address must be IP address of the mediation device.

Configure lawful intercept encryption using CLI

In the following example, an IPSec tunnel is configured between Cisco IOS XE Catalyst SD-WAN device and Media Device Gateway. Media Device Gateway terminates IPSec tunnel and adds a route to Media Device list through the IPSec Tunnel.

In CISCO-TAP2-MIB, source interface is the tunnel interface of the Cisco IOS XE Catalyst SD-WAN devices; destination address is the IP address of the media device.

```
crypto ikev2 diagnose error 1000
crypto ikev2 keyring ikev2_keyring
peer mypeer
address 0.0.0.0 0.0.0.0
pre-shared-key cisco123                      pre-shared key should bee same on media
deviec gateway
!
crypto ikev2 profile ikev2_profile
authentication local pre-share
authentication remote pre-share
dpd 10 3 on-demand
lifetime 14400
keyring local ikev2_keyring
match identity remote address 0.0.0.0 0.0.0.0
!
crypto ikev2 proposal default
encryption aes-cbc-256
group 14 16 19 2 20 21
integrity sha256 sha384 sha512
!
crypto ipsec profile ipsec_profile
set ikev2-profile ikev2_profile
set pfs group16
set transform-set tfs
set security-association lifetime seconds 7200
set security-association replay window-size 256
!
crypto ipsec transform-set tfs esp-gcm 256
mode tunnel
!
interface Tunnel100
no shutdown
ip address 10.2.2.1 255.255.255.0     tunnel address
tunnel source GigabitEthernet1               Cisco XE SD-WAN WAN interface
tunnel destination 10.124.19.57             Media Device Gateway address
tunnel mode ipsec ipv4
tunnel protection ipsec profile ipsec_profile

ip route 10.3.3.0 255.255.255.0 Tunnel100  route MD list traffic through IPSec Tunnel
```

Use the following configuration to configure media gateway to terminate IPSec tunnel:

```
crypto ikev2 proposal default
encryption aes-cbc-256
integrity sha384 sha512 sha256
group 20 16 19 14 21 2
!
crypto ikev2 keyring ikev2_keyring
peer mypeer
address 0.0.0.0 0.0.0.0
pre-shared-key cisco123                          □ pre-shared key, should be same on cEdge
!
crypto ikev2 profile ikev2-profile
match identity remote address 0.0.0.0 0.0.0.0
authentication remote pre-share
authentication local pre-share
keyring local ikev2_keyring
lifetime 14400
dpd 10 3 on-demand
crypto ipsec transform-set tfs esp-gcm 256
mode tunnel
crypto ipsec profile ipsec_profile
set security-association lifetime seconds 7200
set security-association replay window-size 256
set transform-set tfs
set pfs group16
set ikev2-profile ikev2_profile
!
interface Tunnel100
ip address 10.2.2.2 255.255.255.0                 □ Tunnel address
tunnel source GigabitEthernet1                   □ MD GW phy interface
tunnel mode ipsec ipv4
tunnel destination 10.74.5.213                    □ cEdge wan interface
tunnel protection ipsec profile ipsec_profile
!
```

Verify static tunnel with media device gateway

The IPSec tunnel between the Cisco IOS XE Catalyst SD-WAN device and the Media Device gateway is static and is always in the UP state.

Use the following commands to verify static tunnel configuration with the Media Device gateway:

- **show crypto session detail**
- **show crypto ipsec sa**