



Lawful Interception of Traffic

- [Lawful Interception of Traffic, on page 1](#)
- [Configuring Lawful Interception of Traffic on a Cisco Controller \(CLI\), on page 1](#)
- [Viewing and Debugging Lawful Interception of Traffic on a Cisco Access Point \(CLI\), on page 2](#)

Lawful Interception of Traffic

Using the Cisco wireless solution, it is possible to lawfully intercept traffic for monitoring purposes.

Cisco APs create syslog records for traffic and send the records to the controller. Traffic from both IPv4 and IPv6 protocols is recorded. The controller at configured intervals sends these syslog records to the syslog server.



Note The Cisco controller does not store any traffic interception related records.

Restrictions on Lawful Interception of Traffic

- To support IPv6 protocol, enable IPv6 on the controller
- This feature is supported only in Cisco Wave 2 APs operating in Flex + Bridge mode.

Configuring Lawful Interception of Traffic on a Cisco Controller (CLI)

Procedure

- Configure lawful interception by entering this command:
config flexconnect lawful-intercept {enable | disable}
- Configure the syslog for IPv4 and IPv6 host by entering this command:
config flexconnect lawful-intercept syslog host global {ipv4 addr | ipv6 addr}

- Configure the time interval for the syslog to be sent to the syslog server by entering this command:
config flexconnect lawful-intercept timer *timer-value*
- See the lawful interception summary by entering this command:
show flexconnect lawful-interception summary

Viewing and Debugging Lawful Interception of Traffic on a Cisco Access Point (CLI)

Procedure

- See the lawful interception summary by entering this command:
show flexconnect lawful-interception summary
- Debug lawful intercept by entering this command:
debug lawful-intercept flows {all | mac-addr {all | *mac-addr*}}
- Debug lawful-intercept syslog by entering this command:
debug lawful-intercept syslog