Enabling Syslog Messages in Access Points and Controller for Syslog Server

Syslog messages in access points and controllers

A syslog message in access points and controllers is a log communication that

- captures and records operational events generated by each device
- is routed to various destinations, including memory buffers, terminal sessions, device storage, or external syslog servers, and
- allows administrators to configure logging independently on access points and controllers to meet specific network requirements.

Configuring message logging in the IOS XE controller

System Message Logging in Cisco Catalyst 9800 Series Controllers is a platform-independent IOS and IOS XE feature. For more details, see:

- System Message Logging
- Configuration Logger Persistency chapter in *System Management Configuration Guide*
- Logging to Local Nonvolatile Storage chapter in *System Management Configuration Guide*
- Embedded Syslog Manager (ESM) chapter in *System Management Configuration Guide*
- Configuration Change Notification and Logging chapter in *System Management Configuration Guide*

Syslog support for client state change

A syslog client state change event is a network monitoring mechanism that

- records when a wireless client joins, obtains a new IP address, or disconnects from the network,

- captures details such as client IP addresses and access point (AP) names to support network monitoring, and
- provides actionable event logs for operational troubleshooting.

Feature details

A syslog event is generated in these situations:

- When a client enters the RUN state,
- when a client receives a new IP address (IPv4 or IPv6) in the RUN state, and
- when a client in the RUN state is deleted.

Note If syslog support for client state change is enabled and an access point (AP) transitions from standalone to connected, usernames may temporarily appear as null in syslog messages and in client details for 802.1X clients associated with that AP.

This behavior does not affect operations. The system updates usernames automatically after about 30 seconds.

For more information about the IOS XE Controller, see System Message Logging.

Example: Syslog Support for Client State Change

For example, when a client joins a wireless network and obtains a new IP address, a syslog message is generated to record the event, including details such as the client's IP address and the associated AP name.

Configure syslog support for client state change (CLI)

Enable the system to log detailed client state changes for monitoring and troubleshooting.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Enable detailed syslogs for client events.

Example:

```
Device(config)# wireless client syslog-detailed
```

Step 3 Return to privileged EXEC mode.

Example:

```
Device(config)# end
```

The device logs detailed syslog messages whenever a client state changes, aiding in network monitoring and troubleshooting.

Sample syslogs

802.11x authentication

This example shows a client IP update:

```
Oct  1 14:41:27.785 IST: %CLIENT_ORCH_LOG-7-CLIENT_IP_UPDATED:
Chassis 1 R0/0: wncd: Username (dev2), MAC: 0062.xxxx.0077,
IP fe80::262:aff:xxxx:77 101.6.2.119 2001:300:8:0:362:aff:xxxx:77 2001:300:8:0:762:aff:xxxx:77

2001:300:8:0:562:aff:xxxx:77 2001:300:8:0:962:aff:xxxx:77 2001:300:8:0:462:aff:xxxx:77
IP address updated, associated to AP (Asim_06-11) with SSID (dev_abcd_wlan_1)
```

This example shows a client RUN state:

```
Oct  1 14:41:27.779 IST: %CLIENT_ORCH_LOG-7-CLIENT_MOVED_TO_RUN_STATE:
Chassis 1 R0/0: wncd: Username (dev2), MAC: 0062.xxxx.006a, IP 101.xxxx.2.106 associated
to AP
(Asim_06-10) with SSID (dev_abcd_wlan_1)
```

Open authentication

This example shows a client IP update:

```
Sep 18 03:22:35.902: %CLIENT_ORCH_LOG-7-CLIENT_IP_UPDATED:
Chassis 1 R0/0: wncd: Username (null), MAC: 6014.xxxx.c5fb, IP 9.9.xxxx.252
fe80::643c:87c1:xxxx:c1c4 IP address updated,
associated to AP (AP2C5A.xxxx.159A) with SSID (test1)
```

This example shows a client RUN state:

```
Sep 18 03:22:35.257: %CLIENT_ORCH_LOG-7-CLIENT_MOVED_TO_RUN_STATE:
Chassis 1 R0/0: wncd: Username (null), MAC: 6014.xxxx.c5fb, IP 9.9.xxxx.252 associated to
AP (AP2C5A.xxxx.159A) with SSID (test1)
```

This example shows a client delete state:

```
Sep 18 03:24:45.083: %CLIENT_ORCH_LOG-7-CLIENT_MOVED_TO_DELETE_STATE:
Chassis 1 R0/0: wncd: Username (null), MAC: 6014.xxxx.c5fb, IP fe80::643c:xxxx:e316:c1c4
2001:300:42:0:643c:87c1:xxxx:c1c4
2001:300:42:0:xxxx:82ce:1ae4:5a32 9.9.xxxx.252 disconnected from AP (AP2C5A.xxxx.159A) with
 SSID (test1)
```

Configure the syslog server for the controller (GUI)

Enable centralized log management by forwarding controller system logs to a designated syslog server through the controller GUI.

Procedure

Step 1 Choose **Troubleshooting** > **Logs**.

Step 2 Click **Manage Syslog Servers**.

Step 3 In **Log Level Settings**, from the **Syslog** drop-down list, choose a severity level.

Step 4 From the **Message Console** drop-down list, choose a logging level.

Step 5 In **Message Buffer Configuration**, from the **Level** drop-down list, choose a server logging level.

Step 6 In **Size (bytes)**, enter the buffer size. The value can range from 4,096 to 2,147,483,647.

Step 7 In **IP Configuration** settings, click **Add**.

Step 8 From the **Server Type** drop-down list, choose **IPv4**, **IPv6**, or **FQDN**.

Step 9 If you choose **IPv4** or **IPv6**, enter the **Server Address**. If you choose **FQDN**, enter the **Host Name**. Then choose the IP type and the appropriate **VRF Name** from the drop-down lists.

To delete a syslog server, click **x** next to the appropriate server entry under the **Remove** column.

Note
Spaces are not allowed in the host name.

Step 10 Click **Apply to Device**.

Note
When you click **Apply to Device**, the system applies the changes. If you click **Cancel**, the system discards the changes.

After you apply the configuration, log messages are forwarded to the specified syslog server.

Configure a syslog server for a controller (CLI)

Configure the controller to send system and event messages to a remote syslog server for monitoring.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Enter the syslog server IP address and configure its parameters.

Example:

```
Device(config)# logging hostname ipv6
```

Step 3 Enable the facility parameter for syslog messages.

Example:

```
Device(config)# logging facility {auth | cron | daemon | kern | local0 | local1 | local2 |
 local3 | local4 | local5 | local6 | local7 | lpr | mail | news | sys10 | sys11 | sys12 |
sys13 | sys14 | sys9 | syslog | user | uucp}
```

Example:

```
Device(config)# logging facility syslog
```

You can enable these facility parameters for syslog messages:

- **auth** Authorization system.
- **cron** Cron facility.
- **daemon** System daemons.
- **kern** Kernel.
- **local0** to **local7** Local use.
- **lpr** Line printer system.
- **mail** Mail system.
- **news** USENET news.
- **sys10** to **sys14** and **sys9** System use.
- **syslog** Syslog itself.
- **user** User process.
- **uucp** Unix-to-Unix copy system.

Step 4 Set the logging level for the syslog server.

Example:

```
Device(config)# logging trap {severity-level | alerts | critical | debugging | emergencies
 | errors | informational | notifications | warnings}
```

Example:

```
Device(config)# logging trap 2
```

severity-level Refers to the logging severity level. The valid range is from zero to seven.

These are the syslog server logging levels:

- **emergencies** Signifies severity 0. The system is not usable.
- **alerts** Signifies severity 1. Immediate action is required.
- **critical** Signifies severity 2. Critical conditions.
- **errors** Signifies severity 3. Error conditions.
- **warnings** Signifies severity 4. Warning conditions.
- **notifications** Signifies severity 5. Normal but significant conditions.
- **informational** Signifies severity 6. Informational messages.
- **debugging** Signifies severity 7. Debugging messages.

Note
Select a syslog level to view the supported levels. Selecting a level also enables all lower levels.

If you enable the *critical* syslog level, the system also enables lower levels—*alerts* and *emergencies*.

Step 5 Enter privileged EXEC mode.

Example:

```
Device(config)# end
```

Alternatively, press **Ctrl-Z** to exit global configuration mode.

The controller now forwards syslog messages to the specified syslog server as configured.

AP logging to the in-memory buffer and flash

AP always log messages to an in-memory buffer. Once the buffer reaches 40 KB, its contents are automatically written to flash memory, and a new buffer is created.

Administrators can manage and view these logs using AP commands.

- **show logging** command to display the contents of the in-memory logging buffer
- **show flash syslogs** command to list all log files stored in flash, along with other diagnostic files
- **<filename>** command to display the contents of an individual log file stored in flash
- **copy syslogs <filename>** command to transfer a specific syslog file to an external server. To see available options for this command, use **copy syslogs <filename>**

AP logging to terminal

Access points support real-time logging of messages to an active SSH terminal session, which can be enabled or disabled using the **terminal monitor** and **terminal monitor disable** commands.

Administrators can enable real-time logging to an SSH terminal session using the **terminal monitor** command. To disable real-time logging to the session, use the **terminal monitor disable** command. In addition to SSH terminal sessions, APs send a subset of log messages to the serial console, providing another method for real-time monitoring.

Configure AP logging to a syslog server

Use the **syslog** command in the AP join profile to configure the destination IP address for syslog messages and manage which messages are sent based on severity and facility levels.

Configure the syslog host

- Use the **syslog host <IP address>** command to specify the destination IP address for syslog messages.
- By default, the syslog host is **255.255.255.255** , the IPv4 limited broadcast address.

- Configure IP helper addresses on the AP subnet router to forward broadcasts to one or more syslog servers.
- To reset the syslog host to **255.255.255.255** , use either the **default syslog host** or **no syslog host** command.
- To prevent the AP from sending syslog messages entirely, use **syslog host 0.0.0.0** .
- If a subnet contains more than 20 access points, do not log to the broadcast address. This prevents flooding the broadcast domain with log messages. Configure a specific syslog destination IP address.
- If you do not use the AP syslog feature, set the syslog host to **0.0.0.0** by entering the **syslog host 0.0.0.0** command.

Filter messages by severity

- Use the **syslog level <levelname>** command to filter messages based on severity.
- By default, the severity level is **informational** (**severity=6**), which means the system sends all messages except debugging logs to the server.

Filter messages by facility

- Use the **syslog facility <facilityname>** command to filter messages based on the facility code (facility name).
- By default, the facility is **kernel** (**kern** , **code=0**), so the system sends only kernel-related messages.
- To send messages from all facilities, configure the facility as **local7** .
- The configured facility name is included in the facility field of transmitted syslog messages.

Note Most AP log messages use the **kern** facility, while terminal access logs such as SSH and console access use the **auth** facility.

Secured syslog transmission

- Use the **syslog secured** command to enable Transport Layer Security (TLS), as defined in RFC 5425, to transmit syslog messages securely instead of using UDP.
- TLS-based syslog transmission is supported starting with software versions 17.9.6 and 17.12.1 (released in June 2023 and December 2023, respectively).

View syslog settings

To display the current syslog settings for an AP, use the **show capwap client configuration** command.

Configure a syslog server for an AP profile (CLI)

Configure a syslog server for an AP profile.

This ensures access points send system log messages to a specified remote server for central monitoring and troubleshooting.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure an AP profile. Then, enter the AP profile configuration mode.

Example:

```
Device(config)# ap profile ap-profile
```

Step 3 Configure the facility parameter used by syslog messages.

Example:

```
Device(config-ap-profile)# syslog facility
```

Step 4 Enter the Syslog server IP address and parameters to define where the AP profile sends log messages.

Example:

```
Device(config-ap-profile)# syslog host ip-address
```

Step 5 Set the syslog server logging level to determine which messages the AP profile sends.

Example:

```
Device(config-ap-profile)# syslog level {alerts | critical | debugging | emergencies |
errors | informational | notifications | warnings}
```

Example:

```
Device(config-ap-profile)# syslog level
```

The syslog server supports these logging levels:

- **emergencies** —Signifies severity 0. Indicates that the system is not usable.
- **alerts** —Signifies severity 1. Indicates that an immediate action is required.
- **critical** —Signifies severity 2. Indicates a critical condition.
- **errors** —Signifies severity 3. Indicates an error condition.
- **warnings** —Signifies severity 4. Indicates a warning condition.
- **notifications** —Signifies severity 5. Indicates normal, but significant, conditions.
- **informational** —Signifies severity 6. Indicates informational messages.
- **debugging** —Signifies severity 7. Indicates debugging messages.

Note
Select a syslog level to enable it and all lower levels.

If you enable the *critical* syslog level, *alerts* and *emergencies* are also enabled.

Step 6 Return to privileged EXEC mode.

Example:

```
Device(config-ap-profile)# end
```

Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

The syslog server is configured for the specified AP profile. APs that use this profile will send log messages with the selected severity levels to the designated remote server.

Configure the AP syslog settings (GUI)

Set up syslog parameters for access points. This enables monitoring and centralized logging of events.

Procedure

Step 1 Choose **Configuration**, then **Tags and Profiles**, then **AP Join**.

Step 2 Select the APs from the AP list.

The **Edit AP Join Profile** window is displayed.

Step 3 Click the **Management** tab.

Step 4 Select the **Device** tab.

Step 5 In the **System Log** section:

a) From the **Facility Value** drop-down list, select a value.
b) Enter the IP address in the **Host IPv4 or IPv6 Address** field.
c) From the **Log Trap Value** drop-down list, select a value.
d) To enable **Secured**, check the box. To disable **Secured**, clear the box.

Step 6 Click **Update and Apply to Device**

The selected APs are updated with the new syslog configuration, enabling centralized logging according to your specified parameters.

Verify syslog server configurations

Verify global syslog server settings for all APs

To view the global syslog server settings for all access points that joins the controller, use this command:

```
Device# show ap config general
Cisco AP Name : APA0F8.4984.5E48
================================================

Cisco AP Identifier : a0f8.4985.d360
Country Code : IN
Regulatory Domain Allowed by Country : 802.11bg:-A 802.11a:-DN
AP Country Code : IN - India
```

```
AP Regulatory Domain
Slot 0 : -A
Slot 1 : -D
MAC Address : a0f8.4984.5e48
IP Address Configuration : DHCP
IP Address : 9.4.172.111
IP Netmask : 255.255.255.0
Gateway IP Address : 9.4.172.1
Fallback IP Address Being Used :
Domain :
Name Server :
CAPWAP Path MTU : 1485
Telnet State : Disabled
SSH State : Disabled
Jumbo MTU Status : Disabled
Cisco AP Location : default location
Site Tag Name : ST1
RF Tag Name : default-rf-tag
Policy Tag Name : PT3
AP join Profile : default-ap-profile
Primary Cisco Controller Name : WLC2
Primary Cisco Controller IP Address : 9.4.172.31
Secondary Cisco Controller Name : Not Configured
Secondary Cisco Controller IP Address : 0.0.0.0
Tertiary Cisco Controller Name : Not Configured
Tertiary Cisco Controller IP Address : 0.0.0.0
Administrative State : Enabled
Operation State : Registered
AP Certificate type : Manufacturer Installed Certificate
AP Mode : Local
AP VLAN tagging state : Disabled
AP VLAN tag : 0
CAPWAP Preferred mode : Not Configured
AP Submode : Not Configured
Office Extend Mode : Disabled
Remote AP Debug : Disabled
Logging Trap Severity Level : notification
Software Version : 16.10.1.24
Boot Version : 1.1.2.4
Mini IOS Version : 0.0.0.0
Stats Reporting Period : 180
LED State : Enabled
PoE Pre-Standard Switch : Disabled
PoE Power Injector MAC Address : Disabled
Power Type/Mode : PoE/Full Power (normal mode)
Number of Slots : 3
AP Model : AIR-AP1852I-D-K9
IOS Version : 16.10.1.24
Reset Button : Disabled
AP Serial Number : KWC212904UB
Management Frame Protection Validation : Disabled
AP User Mode : Automatic
AP User Name : Not Configured
AP 802.1X User Mode : Global
AP 802.1X User Name : Not Configured
Cisco AP System Logging Host : 9.4.172.116
AP Up Time : 11 days 1 hour 15 minutes 52 seconds
AP CAPWAP Up Time : 6 days 3 hours 11 minutes 6 seconds
Join Date and Time : 09/05/2018 04:18:52
Join Taken Time : 3 minutes 1 second
Join Priority : 1
Ethernet Port Duplex : Auto
Ethernet Port Speed : Auto
AP Link Latency : Disable
```

```
AP Lag Configuration Status : Disabled
AP Lag Operational Status : Disabled
Lag Support for AP : Yes
Rogue Detection : Enabled
Rogue Containment auto-rate : Disabled
Rogue Containment of standalone FlexConnect APs : Disabled
Rogue Detection Report Interval : 10
Rogue AP minimum RSSI : -90
Rogue AP minimum transient time : 0
AP TCP MSS Adjust : Enabled
AP TCP MSS Size : 1250
AP IPv6 TCP MSS Adjust : Enabled
AP IPv6 TCP MSS Size : 1250
Hyperlocation Admin Status : Disabled
Retransmit count : 5
Retransmit interval : 3
Fabric status : Disabled
FIPS status : Disabled
WLANCC status : Disabled
USB Module Type : USB Module
USB Module State : Enabled
USB Operational State : Disabled
USB Override : Disabled
Lawful-Interception Admin status : Disabled
Lawful-Interception Oper status : Disabled
```

Verify syslog server settings for a specific AP

To view the syslog server settings for a specific access point, use this command:

```
Device# show ap name <ap-name> config general
show ap name APA0F8.4984.5E48 config general
Cisco AP Name : APA0F8.4984.5E48
================================================

Cisco AP Identifier : a0f8.4985.d360
Country Code : IN
Regulatory Domain Allowed by Country : 802.11bg:-A 802.11a:-DN
AP Country Code : IN - India
AP Regulatory Domain
Slot 0 : -A
Slot 1 : -D
MAC Address : a0f8.4984.5e48
IP Address Configuration : DHCP
IP Address : 9.4.172.111
IP Netmask : 255.255.255.0
Gateway IP Address : 9.4.172.1
Fallback IP Address Being Used :
Domain :
Name Server :
CAPWAP Path MTU : 1485
Telnet State : Disabled
SSH State : Disabled
Jumbo MTU Status : Disabled
Cisco AP Location : default location
Site Tag Name : ST1
RF Tag Name : default-rf-tag
Policy Tag Name : PT3
AP join Profile : default-ap-profile
Primary Cisco Controller Name : WLC2
Primary Cisco Controller IP Address : 9.4.172.31
Secondary Cisco Controller Name : Not Configured
Secondary Cisco Controller IP Address : 0.0.0.0
Tertiary Cisco Controller Name : Not Configured
```

```
Tertiary Cisco Controller IP Address : 0.0.0.0
Administrative State : Enabled
Operation State : Registered
AP Certificate type : Manufacturer Installed Certificate
AP Mode : Local
AP VLAN tagging state : Disabled
AP VLAN tag : 0
CAPWAP Preferred mode : Not Configured
AP Submode : Not Configured
Office Extend Mode : Disabled
Remote AP Debug : Disabled
Logging Trap Severity Level : notification
Software Version : 16.10.1.24
Boot Version : 1.1.2.4
Mini IOS Version : 0.0.0.0
Stats Reporting Period : 180
LED State : Enabled
PoE Pre-Standard Switch : Disabled
PoE Power Injector MAC Address : Disabled
Power Type/Mode : PoE/Full Power (normal mode)
Number of Slots : 3
AP Model : AIR-AP1852I-D-K9
IOS Version : 16.10.1.24
Reset Button : Disabled
AP Serial Number : KWC212904UB
Management Frame Protection Validation : Disabled
AP User Mode : Automatic
AP User Name : Not Configured
AP 802.1X User Mode : Global
AP 802.1X User Name : Not Configured
Cisco AP System Logging Host : 9.4.172.116
AP Up Time : 11 days 1 hour 15 minutes 52 seconds
AP CAPWAP Up Time : 6 days 3 hours 11 minutes 6 seconds
Join Date and Time : 09/05/2018 04:18:52
Join Taken Time : 3 minutes 1 second
Join Priority : 1
Ethernet Port Duplex : Auto
Ethernet Port Speed : Auto
AP Link Latency : Disable
AP Lag Configuration Status : Disabled
AP Lag Operational Status : Disabled
Lag Support for AP : Yes
Rogue Detection : Enabled
Rogue Containment auto-rate : Disabled
Rogue Containment of standalone FlexConnect APs : Disabled
Rogue Detection Report Interval : 10
Rogue AP minimum RSSI : -90
Rogue AP minimum transient time : 0
AP TCP MSS Adjust : Enabled
AP TCP MSS Size : 1250
AP IPv6 TCP MSS Adjust : Enabled
AP IPv6 TCP MSS Size : 1250
Hyperlocation Admin Status : Disabled
Retransmit count : 5
Retransmit interval : 3
Fabric status : Disabled
FIPS status : Disabled
WLANCC status : Disabled
USB Module Type : USB Module
USB Module State : Enabled
USB Operational State : Disabled
USB Override : Disabled
Lawful-Interception Admin status : Disabled
Lawful-Interception Oper status : Disabled
```