Enabling Syslog Messages in Access Points and Controller for Syslog Server

Information About Enabling Syslog Messages in Access Points and Controller for Syslog Server

The Syslog server on access points and controller has many levels and facilities.

The following are the Syslog levels:

- Emergencies
- Alerts
- Critical
- Errors
- Warnings
- Notifications
- Informational
- Debugging

The following options are available for the Syslog facility:

- auth—Authorization system.

- cron—Cron/ at facility.
- daemon—System daemons.
- kern—Kernel.
- local0—Local use.
- local1—Local use.
- local2—Local use.
- local3—Local use.
- local4—Local use.
- local5—Local use.
- local6—Local use.
- local7—Local use.
- lpr—Line printer system.
- mail—Mail system.
- news—USENET news.
- sys10—System use.
- sys11—System use.
- sys12—System use.
- sys13—System use.
- sys14—System use.
- sys9—System use.
- syslog—Syslog itself.
- user—User process.
- uucp—Unix-to-Unix copy system.

Note For more information about the usage of the syslog facilities and levels, refer to RFC 5424 *(The Syslog Protocol)*.

Configuring Syslog Server for an AP Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *ap-profile* **Example:** `Device(config)# ap profile xyz-ap-profile`	Configures an AP profile and enters the AP profile configuration mode.
Step 3	**syslog facility** **Example:** `Device(config-ap-profile)# syslog facility`	Configures the facility parameter for Syslog messages.
Step 4	**syslog host** *ip-address* **Example:** `Device(config-ap-profile)# syslog host 9.3.72.1`	Configures the Syslog server IP address and parameters.
Step 5	**syslog level** {**alerts** | **critical** | **debugging** | **emergencies** | **errors** | **informational** | **notifications** | **warnings**} **Example:** `Device(config-ap-profile)# syslog level`	Configures the Syslog server logging level. The following are the Syslog server logging levels: • **emergencies**—Signifies severity 0. Implies that the system is not usable. • **alerts**—Signifies severity 1. Implies that an immediate action is required. • **critical**—Signifies severity 2. Implies critical conditions. • **errors**—Signifies severity 3. Implies error conditions. • **warnings**—Signifies severity 4. Implies warning conditions. • **notifications**—Signifies severity 5. Implies normal but significant conditions. • **informational**—Signifies severity 6. Implies informational messages. • **debugging**—Signifies severity 7. Implies debugging messages.

	Command or Action	Purpose
		Note To know the number of Syslog levels supported, you need to select a Syslog level. Once a Syslog level is selected, all the levels below it are also enabled. If you enable *critical* Syslog level then all levels below it are also enabled. So, all three of them, namely, *critical*, *alerts*, and *emergencies* are enabled.
Step 6	**end** **Example:** `Device(config-ap-profile)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Syslog Server for the Controller (GUI)

Procedure

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

Step 2 Click **Manage Syslog Servers** button.

Step 3 In **Log Level Settings**, from the **Syslog** drop-down list, choose a security 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 between 4096 to 2147483647.

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

Step 8 Choose the **Server Type**, from the **IPv4 / IPv6** or **FQDN** option.

Step 9 For Server Type **IPv4 / IPv6**, enter the **IPv4 / IPv6 Server Address**. For Server Type **FQDN**, enter the **Host Name**, 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 When creating a host name, spaces are not allowed.

Step 10 Click **Apply to Device**.

Note When you click on **Apply to Device**, the changes are configured. If you click on **Cancel**, the configurations are discarded.

Configuring Syslog Server for the Controller

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**logging host** {*hostname* | *ipv6*} **Example:** `Device(config)# logging host 124.3.52.62`	Enables Syslog server IP address and parameters.
Step 3	**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`	Enables facility parameter for the Syslog messages. You can enable the following facility parameter for the 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	**logging trap** {*severity-level* | **alerts** | **critical** | **debugging** | **emergencies** | **errors** | **informational** | **notifications** | **warnings**} **Example:** `Device(config)# logging trap 2`	Enables Syslog server logging level. *severity-level*- Refers to the logging severity level. The valid range is from 0 to 7. The following are the Syslog server logging levels: • **emergencies**—Signifies severity 0. Implies that the system is not usable.

	Command or Action	Purpose
		• **alerts**—Signifies severity 1. Implies that an immediate action is required. • **critical**—Signifies severity 2. Implies critical conditions. • **errors**—Signifies severity 3. Implies error conditions. • **warnings**—Signifies severity 4. Implies warning conditions. • **notifications**—Signifies severity 5. Implies normal but significant conditions. • **informational**—Signifies severity 6. Implies informational messages. • **debugging**—Signifies severity 7. Implies debugging messages. **Note** To know the number of Syslog levels supported, you need to select a Syslog level. Once a Syslog level is selected, all the levels below it are also enabled. If you enable *critical* Syslog level then all levels below it are also enabled. So, all three of them, namely, *critical*, *alerts*, and *emergencies* are enabled.
Step 5	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Information About Syslog Support for Client State Change

When a client joins, dissociates, or rejoins a wireless network, the Syslog Support for Client State Change feature enables you to track client details such as IP addresses, AP names, and so on.

A syslog is generated in the following scenarios:

- When a client moves to RUN state.
- When a client gets a new IP (IPv4 or IPv6) address in the RUN state.
- When a client in RUN state is deleted.

Note When Syslog Support for Client State Change feature is enabled, and the AP moves from standalone to connected, you may observe that usernames are null in **syslog messages and in client detail** for the 802.1X clients associated with that AP. You can ignore this behavior, as it does not have any operational impact. The usernames will get updated after 30 seconds.

Configuring Syslog Support for Client State Change (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless client syslog-detailed** **Example:** `Device(config)# wireless client syslog-detailed`	Enables detailed syslogs for client events.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Sample Syslogs

802.11x Authentication

The following 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)
```

The following 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

The following 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)
```

The following 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)
```

The following 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)
```

Verifying Syslog Server Configurations

Verifying Global Syslog Server Settings for all Access Points

To view the global Syslog server settings for all access points that joins the controller, use the following 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
```

Verifying Syslog Server Settings for a Specific Access Point

To view the Syslog server settings for a specific access point, use the following 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
```