

Setting Up System Message Logs (Syslogs) on a CBW Network

Objective

The objective of this article is to set and review logging on a Cisco Business Wireless (CBW) traditional or mesh network.

Applicable Devices | Software Version

- 140AC ([Data Sheet](#)) | 10.4.1.0 ([Download latest](#))
- 145AC ([Data Sheet](#)) | 10.4.1.0 ([Download latest](#))
- 240AC ([Data Sheet](#)) | 10.4.1.0 ([Download latest](#))

Introduction

Cisco Business Wireless access points are 802.11 a/b/g/n/ac (Wave 2) based, with internal antennas. They can be used as traditional standalone devices or as part of a mesh network.

Once your network is set up, things happen that might need attention. To stay aware of these events, you can check the System Message Logs, often referred to as Syslogs.

Being aware of events can help ensure the network runs smoothly and prevent failures. Syslogs are useful for network troubleshooting, debugging packet flow, and to monitor events.

These logs can be viewed on the Web User Interface (UI) of the Primary AP and if configured, on remote log servers. Events are typically erased from the system when rebooted if they are not saved on a remote server.


Setting Up System Message Logs

This toggled section highlights tips for beginners.

Logging In

Log into the Web User Interface (UI) of the Primary AP. To do this, open a web browser and enter <https://ciscobusiness.cisco>. You may receive a warning before proceeding. Enter your credentials. You can also access the Primary AP by entering [https://\[ipaddress\]](https://[ipaddress]) (of the Primary AP) into a web browser.

Tool Tips

If you have questions about a field in the user interface, check for a tool tip that looks like the following: 

Trouble locating the Expand Main Menu icon?

Navigate to the menu on the left-hand side of the screen, if you don't see the menu button, click



this icon to open the side-bar menu.

Cisco Business App

These devices have companion apps that share some management features with the web user interface. Not all features in the Web user interface will be available in the App.

[Download iOS App](#) [Download Android App](#)

Frequently Asked Questions

If you still have unanswered questions, you can check our frequently asked questions document. [FAQ](#)

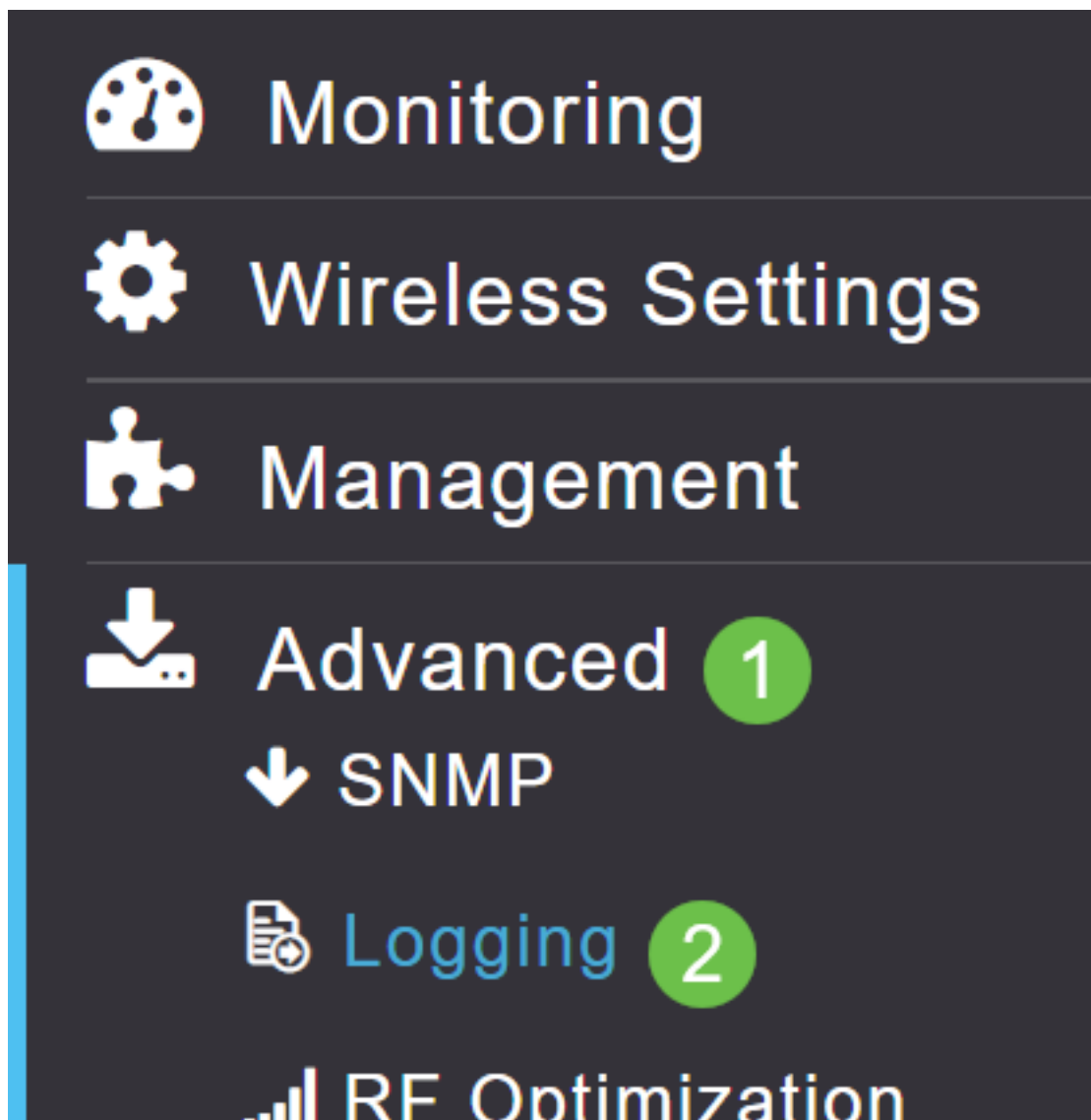
Step 1

Log into the Web UI of the Primary AP. To do this, open a web browser and enter <https://ciscobusiness.cisco>. You may receive a warning before proceeding. Enter your credentials.

You can also access the Primary AP by entering `https://<ipaddress>` (of the Primary AP) into a web browser. For some actions, you can go us the Cisco Business Mobile app.

Step 2

Select **Advanced > Logging**.

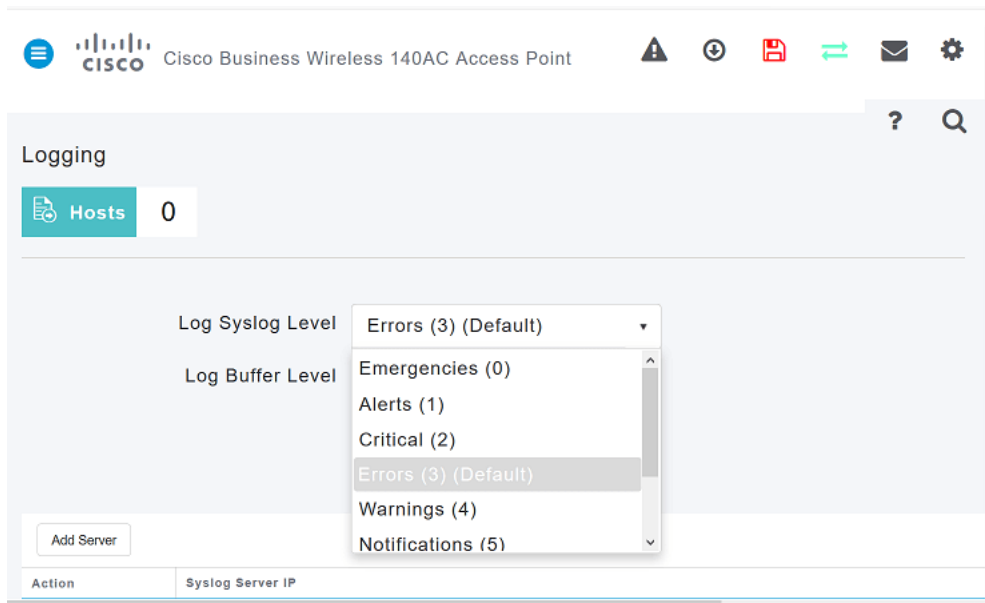


Step 3

Click on the Log Syslog Level. Select from the drop-down menu for the level of notifications. Errors (3) is the default. This means that anything level 3 or more severe is logged.

Shown in the order of severity:

- *Emergencies* (Highest Severity) — This type of message is logged when the device is in a critical situation and immediate attention is required. The system is unusable.
- *Alerts* — This type of message is logged when there is a condition that needs immediate attention.
- *Critical*
- *Errors* (default setting)
- *Warnings*
- *Notifications*
- *Informational*
- *Debugging* (Lowest severity) — This is typically only used when you are actively doing troubleshooting, as you will be flooded with logs pretty quickly.



Step 4

Click **Apply**.

Apply

Step 5

Logs will be displayed when you scroll down the *Logging* page. Click **Clear** if you want to clear the logs. If you do not want to set up a remote Syslog server, go to [Step 8](#).

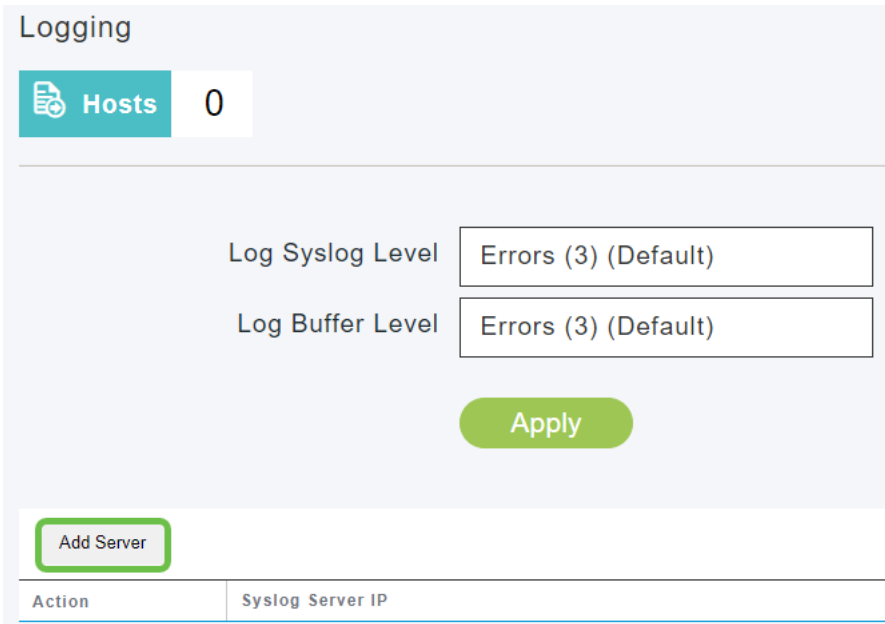
LOGS

1

```
*spamReceiveTask: Mar 11 12:25:30.558: %APF-3-MESH_EXTENDER_AUTHORIZED:
spam_radius.c:288 Wireless Mesh Extender - 68:ca:e4:6e:15:58 authorized by Master AP
*spamApTask0: Mar 11 12:25:30.557: %APF-3-MESH_EXTENDER_ASSOC_REQ:
spam_meshsec.c:1678 Wireless Mesh Extender - 68:ca:e4:6e:15:58 is sending Association
Request to join the network
*spamApTask0: Mar 11 12:24:54.556: %LWAPP-3-AP_DEL: spam_lrad.c:6079
68:ca:e4:6e:ba:60: Entry deleted for AP: 192.168.1.110 (5264) reason : Echo Timer Expiry.
*spamApTask0: Mar 11 12:24:54.551: %WLAN-3-AP_DISCONNECTED: capwap_ac_sm.c:8410
AP68CA.E46E.1558 is disconnected.
*spamApTask0: Mar 11 12:24:54.550: %CAPWAP-3-ECHO_ERR: capwap_ac_sm.c:8373 Did not
receive heartbeat reply; AP: 68:ca:e4:6e:ba:60
*spamReceiveTask: Mar 11 12:23:09.460: %APF-3-MESH_EXTENDER_AUTHORIZED:
spam_radius.c:288 Wireless Mesh Extender - 68:ca:e4:6e:15:58 authorized by Master AP
```

Step 6 (Optional)

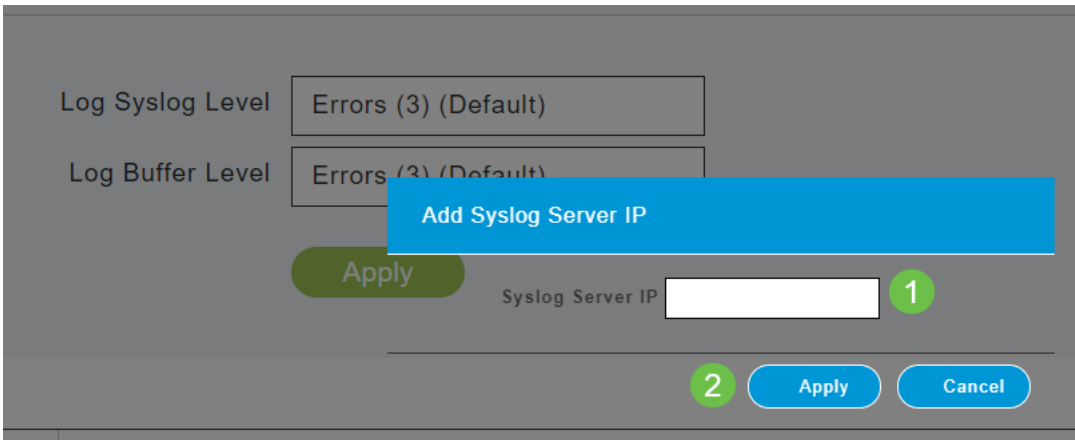
If you would like the logs to be sent to a remote server, click **Add Server**.



The screenshot shows the 'Logging' configuration page. At the top left, there is a 'Hosts' tab with a count of '0'. Below this, there are two dropdown menus: 'Log Syslog Level' and 'Log Buffer Level', both set to 'Errors (3) (Default)'. A green 'Apply' button is centered below these menus. At the bottom left, there is a green 'Add Server' button. Below the 'Add Server' button is a table with two columns: 'Action' and 'Syslog Server IP'.

Step 7 (Optional)

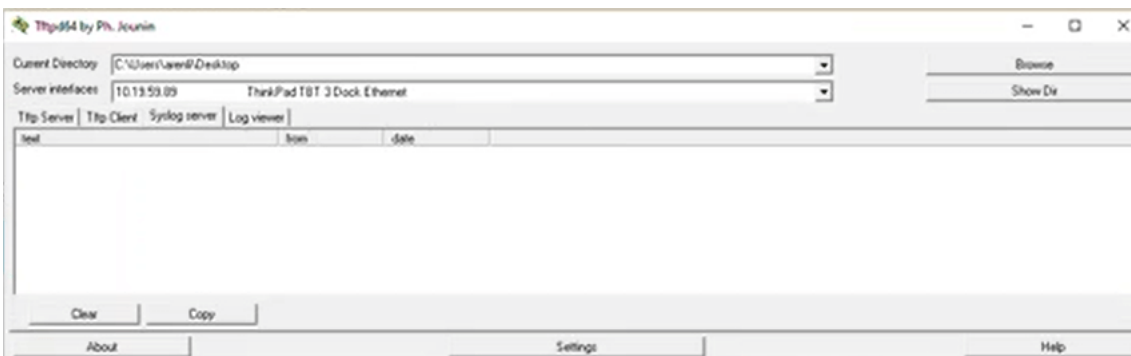
In the *Syslog Server IP* field, enter the IPv4 address of the server to which the Syslog messages should be sent. Click **Apply**.



The screenshot shows the 'Logging' configuration page with a dialog box open. The dialog box is titled 'Add Syslog Server IP' and has a text input field for the IP address, marked with a green circle '1'. Below the input field are 'Apply' and 'Cancel' buttons, with the 'Apply' button marked with a green circle '2'. The background configuration page shows the 'Log Syslog Level' and 'Log Buffer Level' dropdowns set to 'Errors (3) (Default)', and the 'Syslog Server IP' field in the table below.

Step 8

You will need to have a TFTP server open with the Syslog functionality turned on, so the logs can be sent to a file on the server.



Step 9

Be sure to save your configurations by clicking the **Save icon** on the top right panel of the Web UI screen.



System Message Log Example

In this example, the message shows high traffic utilization. If this came up in the syslogs, you would probably want to change the radio frequency channel to one that is less congested for a more stable operating environment.

```
*RRM-DCLNT-5_0: Dec 25 16:51:34:543: %RRM-3-HIGHCHANNEL_UTN: mmLrad.c:7678 Interference is high on AP: APA453.0E1F.E480 [Level: 85] on Radio: 5Ghz(Radio2)
```

Conclusion

You now have access to the system logs. You can go back and change the severity level or add a remote server at any time. This should help keep you up to date on potential issues in the network.

[Frequently Asked Questions](#) [Radius](#) [Firmware Upgrade](#) [RLANs](#) [Application Profiling](#) [Client Profiling](#) [Primary AP Tools](#) [Umbrella](#) [WLAN Users](#) [Logging](#) [Traffic Shaping](#) [Rogues](#) [Interferers](#) [Configuration Management](#) [Port configuration](#) [Mesh mode](#)