Configuring Remote Logging on RV160 and RV260 Routers

Objective

Remote logging can be an effective tool in debugging network issues. Log options on the RV160x and RV260x include: *local*, *email* and *remote server*. This article illustrates the steps in setting up remote logging on an RV160W. Before getting started, we'll provide some additional context to help you determine if this article is for you.

Requirements

- RV160x [Link to Administration Guide]
- RV260x [Link to Administration Guide]
- A previously configured Syslog server or endpoint, with an assigned IP address

Who would use remote logging?

This article would be for a few different types of people. Some are looking to create a data "pipeline" between the RV160x/RV260x and a remote cloud location. Or this could apply to someone sending the logs to an internal network or network endpoint. Thirdly, you may be looking to check in on your network programmatically via a third party provider. The purpose of remote logging is for analysis, monitoring, or storing log contents. With modern data mining techniques, such providers would be able to derrive insight from the logs. Whether or not you're internally or externally storing the logs, the needs of the "pipeline" have different considerations.

This pipeline is very much like a water mainline, it will spray logs wherever you direct it. But to derive value from these logs, some people choose to use a 3rd party to contextualize the logs.

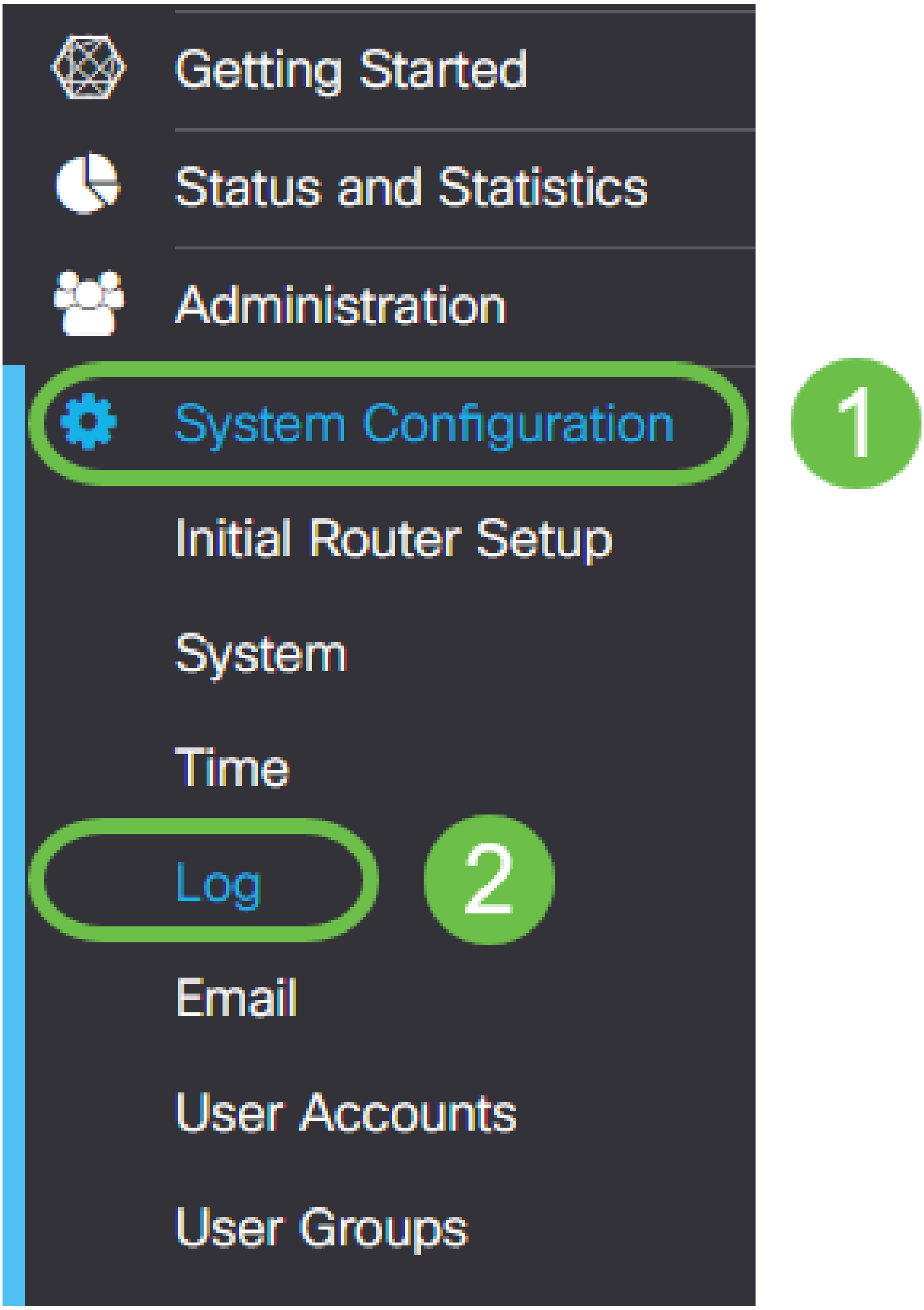
If your Syslog Server isn't yet setup

There are many solutions out there for setting up a remote syslog server. We won't recommend one over the other, here are a couple links to some well options.

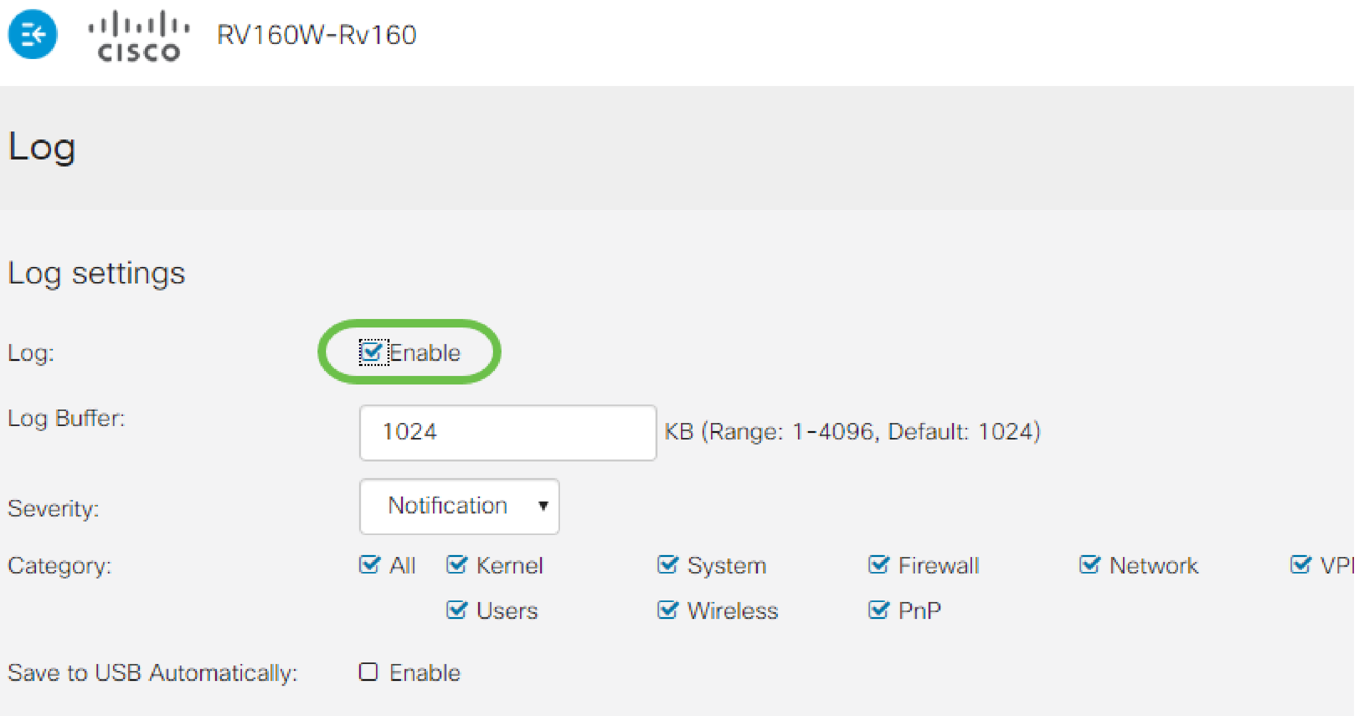
- Cisco Umbrella logs sent to AWS
- Red Hat Syslog Server

Configuring Remote Logging

Step 1. After logging into the router, click **System Configuration > Log**.



Step 2. Click the **Enable** checkbox under the *Log Settings* heading.



RV160W-Rv160

Log

Log settings

Log: ☑ Enable

Log Buffer: 1024 KB (Range: 1-4096, Default: 1024)

Severity: Notification ▾

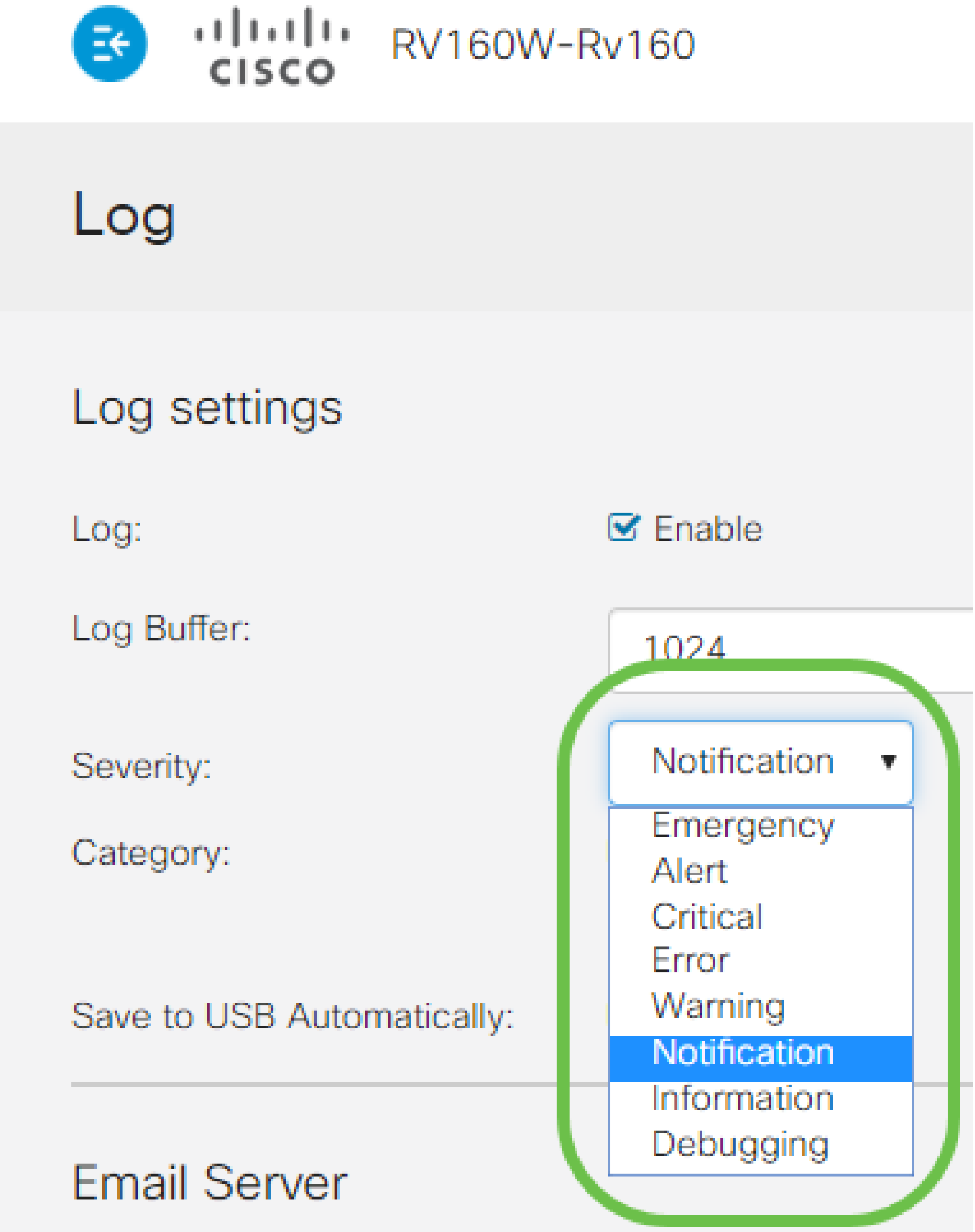
Category: ☑ All ☑ Kernel ☑ System ☑ Firewall ☑ Network ☑ VP
☑ Users ☑ Wireless ☑ PnP

Save to USB Automatically: □ Enable

Step 3. Logs range eight distinct levels of impact. Selecting the appropriate amount of information for your purposes will vary. Keep in mind over time, directories containing logs can grow larger than you may initially anticipate. See below for the list ranked from least to most impact:

1. Debugging - Logs the most amount of information, for troubleshooting.
2. Information - Non-performance impacting details.
3. Notification - Normal but significant condition.
4. Warning - functional but in danger of toggling into error mode.
5. Error - Function or feature is unavalable because of error.
6. Critical - crucial conditions.
7. Alert - Immediate action is required.
8. Emergency - Device is unusable or unreachable.

Note: Only enable Debugging if you are actively working with the logs.



RV160W-Rv160

Log

Log settings

Log: ☑ Enable

Log Buffer: 1024

Severity: Notification

Category:

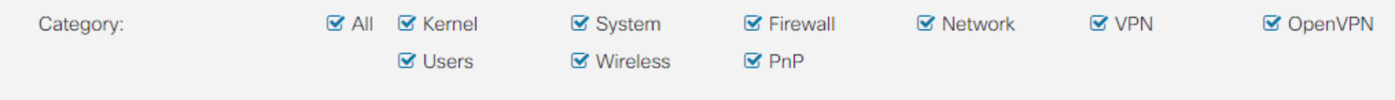
Save to USB Automatically:

Email Server

Note: Be selective about the settings selected here, but you can dial it into your needs via experimenting.

Step 4. Further decisions in this section require the same amount of judcious review. All categories selected is by default, which is what we've selected.

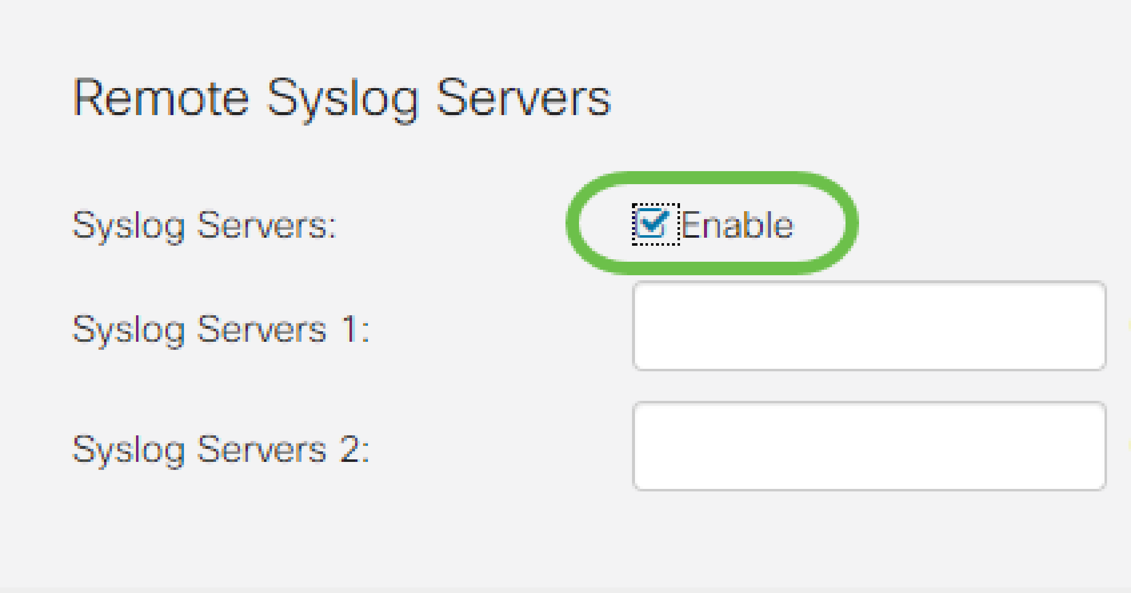
1. Kernel
2. System
3. Firewall
4. Network
5. VPN
6. OpenVPN
7. Users
8. Wireless
9. PnP



Category: ☑ All ☑ Kernel ☑ System ☑ Firewall ☑ Network ☑ VPN ☑ OpenVPN
☑ Users ☑ Wireless ☑ PnP

Note: When selecting which categories if you're using a third party to analyze the logs, check their documentation for which categories to include.

Step 5. Scroll to the bottom of the page (if applicable). Then click the **Enable** checkbox below the *Remote syslog Servers* heading.



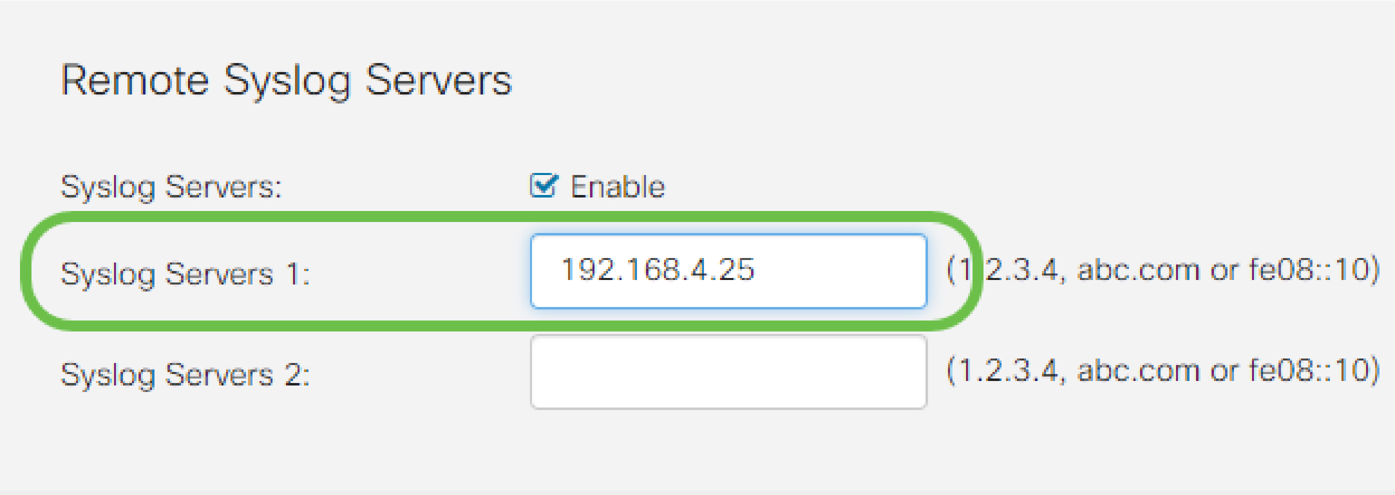
Remote Syslog Servers

Syslog Servers: ☑ Enable

Syslog Servers 1:

Syslog Servers 2:

Step 6. Enter the **IP Address** of the remote server.



Remote Syslog Servers

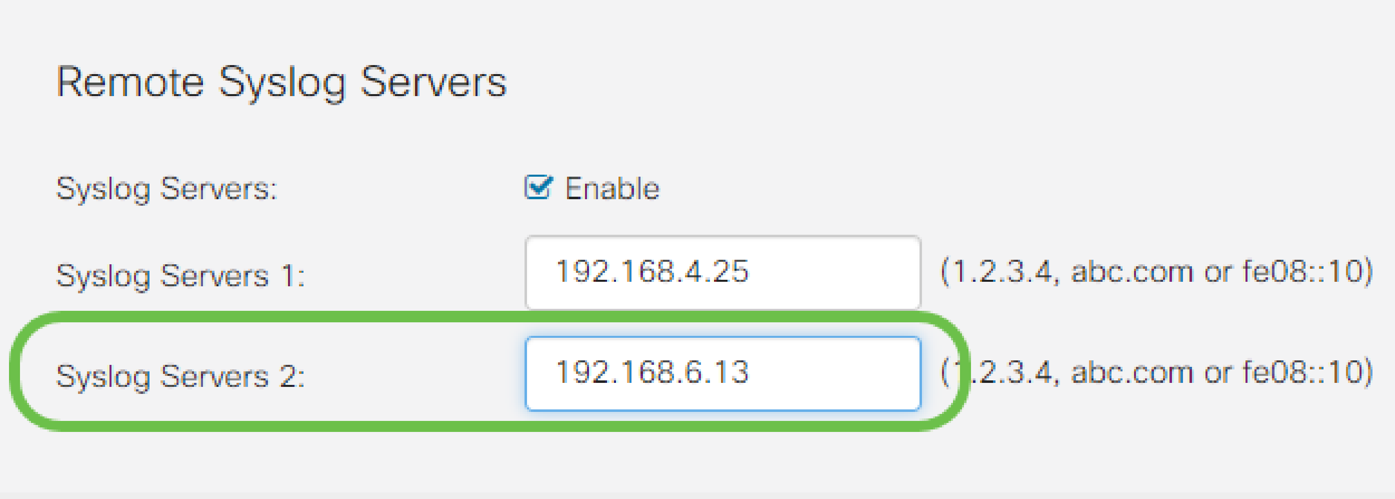
Syslog Servers: ☑ Enable

Syslog Servers 1: 192.168.4.25 (1.2.3.4, abc.com or fe08::10)

Syslog Servers 2: (1.2.3.4, abc.com or fe08::10)

Note: The remote logging server must be a valid endpoint for the delivery of syslog files.

Step 7. (Optional) For redundancy, add an additional IP address.



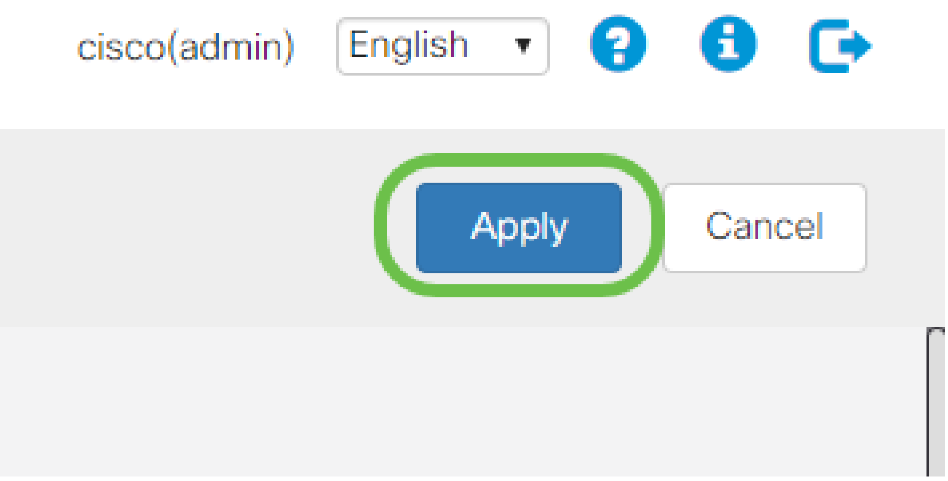
Remote Syslog Servers

Syslog Servers: ☑ Enable

Syslog Servers 1: 192.168.4.25 (1.2.3.4, abc.com or fe08::10)

Syslog Servers 2: 192.168.6.13 (1.2.3.4, abc.com or fe08::10)

Step 8. Click **Apply** to complete the configuration.



Step 9. Be sure to **Save** the configuration from **running config > startup config**.

Conclusion

In this configuration guide, we reviewed directing the RV160x/RV260x routers to send logs to an endpoint via IP address. Note that logs are only generated after activation, they are not generated in a retroactive method.