

Enable or Check Syslog/CEF on SonicWall

1. Log in to SonicWall UI

- Open a web browser
- Go to your SonicWall's IP (e.g., `https://192.168.1.1`)
- Login with your admin credentials

2. Navigate to Log Settings

- Go to:
 - Log > Syslog
 - (On older firmware: `Log > Syslog > Syslog Servers`)
- You'll see the list of configured **Syslog Servers**

3. Check Syslog Server Configuration

- Make sure the following are set:
 - **Syslog Server IP Address:** should be the IP of the **Elastic Agent** host
 - **Port:** default is **514** for UDP, or **6514** for TCP/TLS
 - **Syslog Format:**
 - Can be set to **Default**, **Syslog**, or **CEF** (Common Event Format)
 - For Elastic integrations, **Syslog** or **CEF** is typically supported

4. Enable Log Categories

- Still under **Log > Syslog**, click **Syslog Settings**
- Ensure that **Important log categories** are **enabled for syslog**, like:
 - **Firewall**
 - **VPN**
 - **System**
 - **User Activity**
 - **Connection dropped**
- Set **Alert level** or **Priority**: e.g., **Information** or **Notice**

5. If Using CEF Format (For Elastic Agent CEF Integration)

- Some SonicWall models support **CEF log format**:
 - Go to **Log > Syslog**
 - Look for an option like **"Syslog Format"** or **"Use CEF"**
 - Enable **CEF output**
- *Note:* Not all SonicWall devices support native CEF.

6. Advanced Settings (Optional)

- Under **Log > Syslog Settings**, check:
 - Syslog Facility (can be left as default: `Local0` or `Local4`)
 - Use **Syslog over TLS** if required, and provide the correct certs

7. Save and Apply

- Click **Apply** or **Accept** to confirm changes

- Ensure the firewall can reach the Elastic Agent on the configured port
-

Revision #2

Created 7 July 2025 23:48:52 by Jeff Saguing

Updated 8 July 2025 00:05:03 by Jeff Saguing