Proxy Device Uploads

Proxy Device Uploads

Upload telemetry data in log files from proxy devices such as the Cisco Secure Web Appliance (formerly Web Security Appliance or WSA) and Blue Coat ProxySG to the global threat alerts system for analysis.

Step 1 Click the gear icon in the upper-right corner of the page, and select **Device Accounts** to open the setup wizard.

Note If there's already at least one existing device account, the setup is skipped and the Device Accounts page is displayed.

Step 2 When you're ready to start the setup wizard to add a device account, click **Let's Get Started**.

Step 3 Choose how the telemetry data is uploaded from the device by selecting either automatic or manual upload from the dropdown. The global threat alerts system supports only one upload method at a time; they cannot be combined.

Note To switch from automatic to manual uploading, all proxy devices must first be removed from the automatic uploading configuration.

Step 4 If you selected the automatic upload method, choose what protocol is used to transfer the log files by selecting either **SCP** or **HTTPS**.

a) Enter a name for this device, and click **Add Account**.

b) If you selected SCP:

- Copy the information (host, port, directory, username) to paste into your Cisco WSA configuration. For security reasons, the information is displayed only once.
- For details on how to configure your Cisco WSA, see Configure Cisco Secure Web Appliance to Upload Log Files to Cisco Global Threat Alerts.
- Once the Cisco WSA Management Console returns a public SSH key, copy and paste the public SSH key into the device account.
- Click **Finish**.
- Optionally, you can enter the public SSH key later by navigating to the Device Accounts page and clicking the device.

c) If you selected HTTPS:

- Copy the information (host, port, path, username, password) to paste into your Blue Coat ProxySG configuration.
- For details on how to configure your Blue Coat ProxySG, see Configure Blue Coat ProxySG to Upload Log Files to Cisco Global Threat Alerts.
- Click **Finish**.

Step 5 If you selected the manual upload method:

a) Validate the format of your log file(s). Follow these preparation guidelines:

- W3C log files created by Cisco WSA and Blue Coat proxies are supported.
- All log files must be compressed in GZip (*.gz) format.
- Each log file must be smaller than 1 GB. A log file bigger than 1 GB should be divided into multiple, smaller files. Ensure separate time intervals do not overlap and every file contains the same correct header.
- Total time interval covered by the log files should be greater than two days.
- Each log file must be for a specific, non-overlapping time interval.
- Each log file must contain log entries in ascending time order; older entries before newer entries.
- Log files should be sorted alphabetically/numerically and uploaded in order according to time; older files should be uploaded before newer files. Within a single upload, the uploading component automatically sorts the files. If you upload multiple times, ensure you always upload newer data than before. If the naming convention used by default in the proxy log files is retained, the file names are already correctly sorted.
- Data older than previously uploaded data will not be processed.
- The content of the log files must match certain criteria to be valid for uploading.
  - We offer you a Log Validation Tool to check your log files before uploading.
  - Copy-and-paste the beginning 20 lines of your log file into the Log Validation Tool to check for errors.
  - Any errors are displayed, and while you correct them, the tool will automatically continue to check for errors.

b) Click either **Add files** to select log files to be uploaded or drag-and-drop log files into the upload box.

Note Click **Clear files** to clear all files added to the upload box.

c) Clicking **Start upload** uploads the selected log files to the global threat alerts system for analysis. Allow the global threat alerts system some time before seeing results.

Note To minimize the risk of dropping data, the global threat alerts system starts processing the uploaded data after 5 hours. This gives you time to complete all your uploads and ensure everything is in place and in proper order before processing starts.

Caution Trying to switch from manual to automatic immediately aborts all uploading and stops processing of uploaded data. All uploaded data is discarded.

Note Closing or navigating away from the page will stop any current file upload.

Note You cannot use automatic uploading unless you first stop all manual uploading. If the switch is made before all the data is processed, some analysis data may be lost from the transition. To ensure the system does not drop any data, perform the switch after 24 hours after the last manual upload.

What to do next

The Device Accounts page lists the proxy devices along with their information. The Status column shows the status of each device:

- New—Incomplete configuration for SCP, may be missing public SSH key
- Provisioning—Account in the process of being provisioned, not yet ready
- Ready—Account successfully created
- Error—Hover cursor over status to display a popup message explaining the error

From this overview page, you can add more device accounts, or click any device to remove it, enter a public SSH key, or troubleshoot.

Although it is possible to share an account between multiple devices or upload processes, we recommend you use a separate account for each device to minimize the possibility of filename conflicts and simplify troubleshooting upload problems.

When your device account is ready, click to view the **Confirmed** or **Detected** pages for insight into any suspicious activities in your network.

Note Data is typically available within two to three days after provisioning is complete.

Proxy Device Uploads