Threats Tab

- Dashboard, on page 1
- Confirmed Threats, on page 1
- Detected Incidents, on page 3
- Incident Details, on page 5
- Proxy Device Uploads, on page 7

Dashboard

The CTA Dashboard page provides an overview of your network health and what threats are affecting it:

- Health Status. Shows an overall summary of threats discovered in your network by their risk level. Unresolved users are grouped by risk category. Note that a high number of lower risk threats may lead to more serious threats over time.

- Relative Threat Exposure. Threat exposure based on your number of incidents and their risk level, compared to other companies within your same sector, similarly sized companies, and all companies globally.

- Specific Behaviors. High-level breakdown of the detected threats and unresolved behaviors in your network.

- Highest Risk. Unresolved incidents that currently pose the highest risk to your network and require your immediate attention.

- Top Risk Escalations. Unresolved incidents that have recently showed an increase in risk.

Confirmed Threats

The Confirmed page shows information about confirmed threat campaigns in your network.

- Threats spanning across multiple users
- 100% confirmed breaches, no false positives
- Ready for fast remediation, directly actionable
- Cisco Collective Security Intelligence, additional information provided for context
Threat campaigns are listed in the vertical panel at the right of the page.

- At the top of the threat list panel are check boxes for the incident states: Triage, Investigating, Remediating, and Resolved. Use these four check boxes to filter what threats are shown in the vertical panel. For example, uncheck the Resolved box to hide threats containing incidents marked in the Resolved state.

- Threats are sorted top-to-bottom by risk level with the highest-risk threat at the top.

Click a threat to view its information to the left of the vertical panel.

- **#Cxxxxx**—Incidents detected with correlated behavior are grouped into a threat cluster. Each threat is then labeled with a unique hash-tag group name.
  - **Risk level**—Number from a scale of 1 to 10 representing the risk of the threat impacting your network. A higher number indicates a higher risk. We recommend you prioritize your analysis by investigating higher risk threats and the incidents clustered within them before lower risk threats.
  - **Confidence**—Percentage indicating the precision of the detection category. A higher number indicates a higher confidence that the symptoms are correctly classified and the incident represents a valid threat on your network.
  - **Incidents Bar**—Horizontal, graphical bar showing the number of incidents clustered in the threat.
    - Number of incidents are broken down per incident state, corresponding to the varying shades of the four incident state boxes.
    - For example, in the bar shown here, there are 17 incidents in the Triage state, 12 incidents in the Investigating state, 21 incidents in the Remediating state, and 80 incidents in the Resolved state.

- **Affecting**—Number of your users affected by this threat within the past 45 days. Also shows number of users affected at other companies to help you determine if the threat is targeted.

- **Occurrence**—When this behavior occurred, when it was first seen, and when it was last seen.

Below the threat summary are sections showing more details on the selected threat:

- **Description of the threat and recommended actions to remediate.**
- **List of affected users and graph showing number of users exhibiting malicious behaviors over time.**
- **Example web requests representing threat behavior in your network.** If the URL contains an encoded part, the system attempts to show the decoded content here.
- **Cisco Cloud Web Security malware blocks observed for users in your network affected by this threat.**
- **AMP Threat Grid Global Intelligence**—Common endpoint content security signatures and behaviors associated with global traffic samples of the threat.
  - Common files appearing in global threat samples that may be present on endpoints, percent chance these files are created or modified by malware on endpoints, and severity of the file type
  - Common endpoint behaviors associated with similar threats seen in samples from AMP Threat Grid
Detected Incidents

The CTA system monitors your web proxy logs but does not inspect the content of the communications. The CTA system focuses on identifying malicious web browsing behaviors and presents incidents derived from the behavioral symptoms of an infection. The Detected page shows an overview of detected incidents which may be suspected threats, including noncorrelated CTA incidents and AMP retrospective incidents. You can also view the correlated CTA incidents that were grouped into verified threats on the Confirmed page.

- **Incident**—Type of dominant behavior detected on an individual, including its Risk and Confidence levels, and whether it's part of a cluster or confirmed threat. Clusters are a collection of incidents that have similar malware symptoms.

  - **Risk**—Number from a scale of 1 to 10 representing the risk of the incident. A higher number indicates a higher risk. We recommend you prioritize your analysis of incidents by investigating higher risk incidents before lower risk incidents.

  - **Confidence**—Percentage number indicating the precision of the detection category. A higher number indicates a higher confidence that the symptoms are correctly classified and the incident represents a valid threat on your network. Applies to CTA incidents only.

- **User Identity**—User ID and IP address of the affected user.

  - IP addresses can be reassigned to multiple users over time, so the CTA system models by user. This important system enhancement provides more consistent results.

  - A user may be assigned more than one IP address over time. The CTA system tracks these assignments and displays all the IP addresses that have been assigned to the user during the selected time period.

- **IP Reputation**—The rating of the remote server contacted represents an aggregation of known sources the user has communicated with during each incident. The rating is not used in the Anomaly Detection Engine for detection. Instead, the rating is provided to the security analyst as an informational aid to better understand the (global intelligence) context in which the detection of an incident occurred.

  - **Red**—Number of remote servers contacted with a poor IP reputation rating (–10 to –6).

  - **Orange**—Number of remote servers contacted with no record in the Global Intelligence database or a neutral rating (–5 to +5).

  - **Green**—Number of remote servers contacted with a good IP reputation rating (+6 to +10).

- **Duration**—How long and when this behavior occurred. Also refer to First Seen and Last Seen columns.

- **State**—Incident marked as triage, reoccurring, investigating, remediating, resolved, a false positive, or to be ignored.

- **Anomaly Types**—Types of anomaly detected in this incident including risk factor (critical, high, medium, low). Each incident is formed by a number of anomalies. Each anomaly represents malware behavioral symptoms. Hover over a cell to show all the anomaly types associated with that incident. Anomaly types are sorted top-to-bottom by risk factor with the most critical at the top.
• **Last Updated**—When this incident was created or when some ongoing traffic was last added.

### Filtering Incidents

You can filter which incidents are shown by:

- **Date selector**—Click each field to open a calendar and choose the start (From) and end (To) dates.
  - By default, the previous 45 days are shown.
  - The maximum date range is 45 days.
  - The available date range is the previous 45 days.
  - You can also quick click **1 day, 3 days, 7 days, 30 days, or 45 days**.

- **Search field**—Enter any username, client IP address, or incident name (no regular expressions or wildcards), and click the **Filter** button.

- **Show**—There are check boxes to show AMP and/or CTA incidents, confirmed and/or low confidence incidents, and tabs to show incidents by what state they're in:
  - **Triage**—(Default) Incidents that are new or reoccurring and need to be investigated.
  - **Investigating**—Incidents under investigation and being worked on.
  - **Remediating**—Incidents in the process of being resolved, devices pending cleaning.
  - **Resolved**
    - **Remediated**—Incidents that have been remediated, devices have been cleaned.
    - **False Positives**—Incidents assessed to be false positives.
    - **Ignored**—Incidents marked to be ignored and not investigated. For example, incidents for devices in a guest Wi-Fi zone.

- **All**—All incidents regardless of state or marking.

---

**Note**

Incidents can be marked by using the drop-down list on the Incident Details page. See **Incident Details, on page 5**.

### Settings

Click the global settings menu icon (sandwich) in the upper-right corner of the page:

- **Email Notifications**—Enter email addresses to be sent a summary of new and updated incidents every 24 hours.

- **CTA STIX/TAXII Service**—Use the STIX/TAXII service to pull information on incidents detected by CTA down to your SIEM client for further analysis, incident response, and data archival. See **CTA STIX/TAXII Service**
• **Device Accounts**—Upload telemetry data in log files from one or more source proxy devices to the CTA system for analysis. To access this service, the External Telemetry feature must be enabled and provisioned for your company. If you do not have the External Telemetry feature, contact your Cisco Cloud Web Security account team. See [Proxy Device Uploads](#) on page 7.

• **Define Ignored Networks**—Hide alerts by listing which IPv4 addresses and network ranges to ignore. This is useful for filtering unnecessary alerts such as alerts from a guest network or other, less critical pieces of your network. Enter IPv4 addresses for hosts, networks, or IPv4 address ranges (for example: 10.100.10.1, 10.100.10.0/24, 10.100.10.1-10.100.10.254) that you want hidden from the list of incidents.

• **Release Notes**—Summarizes updates, changes, and fixes per release.

In the table header and below the global settings menu button:

- Click the download button to export the incidents (from the current filter displayed) to a CSV file on your device.
- Click the page settings button to select what columns are displayed.
- Click the sorting arrow in any column header to sort the table rows according to the information in that column.
- Resize any column width by dragging the line between the column header cells.
- Reorder table columns by selecting a column (click on its header) and once the pointer changes to crossing arrows, drag and drop the column by its header to a new location in the table.

To further investigate an incident, hover in the row of that incident and the row becomes highlighted. Click in the row to open the incident details page. Alternately, you can open the incident details page in a new window by right-clicking the incident and choosing **Open incident in a new window**.

### Incident Details

An incident typically consists of multiple activities or types of suspicious behavior. There are three main sections on the incident details page.

### Incident Header

The first main section is the incident header:

- **Incident Classification**—Type of dominant behavior detected, including its Risk and Confidence levels.
  - **Risk**—Number from a scale of 1 to 10 representing the risk of the incident infecting the network. A higher number indicates a higher risk. Therefore, we recommend you prioritize your analysis of incidents by investigating higher risk incidents before lower risk incidents.
  - **Confidence**—Percentage number indicating the precision of the detection category. A higher number indicates a higher confidence that the symptoms are correctly classified and the incident represents a valid threat on the network. Applies to CTA incidents only.

- Use the drop-down list to mark the incident as triage, investigating, remediating, resolved as threat, resolved as false positive, or resolved as ignored. This marking serves two main purposes. One, it categorizes incidents to aid the workflow of incident management and analysis. Two, it becomes part of
community feedback that Cisco uses to improve the detection algorithms. Remember to mark the incident after investigation. In the table of listed incidents, the marking is shown in the State column.

- **Affecting**—User ID and IP address of the affected user. Also shows the operating system and whether the incident relates to a proxy.

  | Note | If the text is encrypted, the field values were anonymized by WSA 11.5 when its log files were pushed to CTA for analysis. For information on how to deanonymize the encrypted text, see Configure WSA to Upload Log Files to CTA System.

- **Occurrence**—When this behavior occurred and its history.

  | Note | The SHA-256 hash of any malicious files found is also listed here. Hover over the red skull-and-crossbones icon and click View full report to open the sandbox report in a new window. See Sandboxing.

  | Note | Click View web traffic history to open a new page that shows the web browsing history of this user in a Cisco ScanCenter WIRe (Web Intelligence Reporting) report.

### Parallel Coordinates

The second main section is the parallel coordinates graph showing relationships between time, anomaly, domain, IP address, and autonomous system:

- At-a-glance shows information about the anomalies in the incident and their associations.
- Hover over each coordinate node in the line graph to show its interconnected information.
- Domains that are targets for persistent connections are highlighted in bold with a PERS indicator.
- Click the drop-down icon next to a domain name for more details.
- IP address includes country location and IP reputation.
- Click the drop-down icon next to an IP address for more details.
- Can be used to filter web flows by selecting and clicking one or more nodes. The associated web flows are then listed in the table below the graph.
- Select critical, high, medium, and/or low to display flows filtered by anomaly risk factor.

### Web Flow Requests

The third main section is a table listing details of the web flow requests:

- **Client IP**—IP address used on client.
- **Client Port**—TCP/UDP port used on client.
• **Server IP**—IP address used on server. Includes country flag of server location, if known, and the IP reputation score of the server. A red box next to the server indicates a negative IP reputation for that server. Domain names are included. The negative IP reputation could indicate suspicious communication from a domain operated by an attacker.

• **Server Port**—TCP/UDP port used on server.

• **Bytes Up**—Amount of data sent to server.

• **Bytes Down**—Amount of data received from server.

• **Header Content Type**—Content type in the HTTP header sent by the remote server.

• **Body Content Type**—Content type detected in the response body. Can differ from Header Content Type in cases where, for example, the malicious host tries to get through proxy or firewall filtering rules.

• **URL**—Unified Resource Locator of the server accessed by the client. Hover over the URL, and if the URL contains an encoded part, the system attempts to show the decoded content here. Often reveals commands and data passed through.

• **Referrer**—HTTP header field identifying the address of the URL that linked to the resource being requested.

• **HTTP Status**—HTTP status code returned from the server. A red box with an "x" next to the status code indicates that the flow was blocked by the Web proxy.

• **Timestamp**—Time connection started.

• **Duration**—How long the event lasted.

• **User Agent**—Type of browser used during activity.

• **Category**—Site category (for example, gambling and social sites).

• **Filename**—Name of file that was downloaded (AMP-specific field).

• **SHA-256**—Secure Hash Algorithm SHA-256 computed for the file (AMP-specific field). If a sandbox report of the file is available, an icon appears next to the SHA-256. Hover over the icon and click **View full report** to open the sandbox report in a new window. A red skull-and-crossbones icon indicates that the file was found to be malicious. See Sandboxing.

In the Search field, enter any client IP address, server IP address, URL, or SHA value (no regular expressions or wildcards), and click the **Filter** button.

Click the page settings button to select what columns are displayed. Click the sorting arrow in any column header to sort the table rows according to the information in that column. Reorder the columns by clicking and dragging by their headers.

At the bottom of the page below the table is a single row footer showing summary statistics for the selected web flows: traffic amount, percentage blocked, number of requests, total duration, user agents, no referrer percentage, and HTTP status code.

### Proxy Device Uploads

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

**Procedure**

**Step 1** Click the **Threats** tab.
Step 2  Click the global settings menu 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 3  When you're ready to start the setup wizard to add a device account, click **Let's Get Started**.

Step 4  Choose how the telemetry data is uploaded from the device by selecting either automatic or manual upload from the dropdown. The CTA 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 5  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 its **Configuration Guide**.
   
   • 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 its **Configuration Guide**.
   
   • Click **Finish**.

Step 6  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 CTA system for analysis. Allow the CTA system some time before seeing results.

**Note** To minimize the risk of dropping data, the CTA 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. For more information, see Threats Tab, on page 1.

**Note**

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