

# Cisco SecureX Tiles List

---

**First Published:** 2020-06-26

**Last Modified:** 2022-10-13

## Overview

SecureX connects Cisco's integrated security portfolio and your entire security infrastructure to unify visibility, enable automation, and strengthen security across your network. The result is simplified security, built into the solutions you already have. The **Tiles** pane in the center of the SecureX dashboard presents metrics and data from your integrated products to provide visibility across your security environment and accelerate threat response. After you've added your integrations to SecureX, the tiles that are provided by the products are available for you to add when you customize your dashboard. This document is a supplemental list of tiles and their descriptions that may be available in SecureX.



---

**Note** While we periodically update this tiles list, it may not always reflect the complete list of tiles in every product integrated with SecureX.

---

## Cisco Defense Orchestrator (CDO)

Tile Name	Description
CDO Device Summary	CDO device status summary.
CDO Objects and Policies	CDO objects and policies summary.
CDO VPN	CDO VPN summary.
CSDAC - Elements	CSDAC elements summary.
CSDAC - Source Connectors	CSDAC connectors by type and status.
CSDAC - Destination Adapters	CSDAC adapters by type and status.
CSDAC - Dynamic Objects	CSDAC dynamic objects and count of mappings.

## Cloud Mailbox

Tile Name	Description
Messages by Direction	Shows your total email traffic by direction. Mail is divided into Outgoing, Mixed, Internal, and Incoming.
Malicious & Phishing	Shows a snapshot of messages that were determined to be Malicious or Phishing.
Spam	Shows a snapshot of messages that were determined to be Spam.
Graymail	Shows a snapshot of messages that were determined to be Graymail.

## Duo

Tile Name	Description
Duo Trust Monitor	Shows statistics from Duo Trust Monitor.

## Firepower Threat Defense (FTD)

For important information about this integration, and to configure your system to send events from FTD devices to SSE, see the *Cisco Firepower and SecureX Integration Guide*, available at <https://cisco.com/go/firepower-securex-documentation>.

### Important Information about Tiles

Tiles showing metrics for events show events that have been sent from FTD devices to Security Services Exchange (SSE) within the past 7 days.

To ensure that you see the correct set of events, you must correctly configure auto-promotion options in Security Services Exchange. For details, see the online help in SSE. To access SSE, you can click a summary value in the Event Summary tile.

Some tiles are applicable only to systems managed by Firepower Management Center (FMC), not to deployments managed by Firepower Device Manager (FDM).

Some links from these tiles take you to your FMC appliance. As long as your browser can connect to your internal network, you can access your FMC from within SecureX. (SecureX does not need to connect to your corporate network.)

To cross-launch FMC from the tiles in SecureX, the FMC's name must be a Fully Qualified Domain Name (FQDM). To change the name of your FMC, go to **System > Configuration > Information** in the FMC web interface and modify the **Name** field.

### Event Summary Tile

This tile summarizes FTD events in SSE within the timeframe selected, up to 7 days.

You can view event details in Security Services Exchange (SSE) by clicking metrics in this tile. SSE will open in a separate browser window.

### Incident Promotion Reason Tile


This tile summarizes FTD events in Security Services Exchange (SSE) that have been promoted to incidents within the timeframe selected, up to 7 days.

The tile displays the reasons that events were promoted to incidents, which can be:

- Automatically by the system (Talos Disposition)

Intrusion events that involve an IP address with a poor Talos IP reputation score are automatically promoted to incidents. If you have enabled auto-promotion of malware events in SSE, this metric also includes malware events with a poor source IP reputation score.

- Automatically based on your organization's configured auto-promote settings in SSE.

These settings are located in SSE by clicking **Cloud Services > Eventing >  > Auto-Promote Events**. Security Intelligence categories (DNS, URL, and IP addresses) include events promoted based on matches based on Talos threat intelligence data and, if SSE is configured to automatically promote events based on custom security intelligence lists and feeds, those events as well.

The other configurable auto-promotion reasons are Intrusion Rules Category, Malware Threat Score, and Custom IP Address.

- Manually by a user from the Events page in SSE. (User Promoted)

Select or deselect checkboxes to modify the graph display.

For more information about promoting events to incidents, see the online help in SSE.

### Talos IP Reputation Tile

This tile summarizes the Talos reputation scores of the public IP addresses associated with intrusion and malware events sent from FTD to Security Services Exchange (SSE) within the timeframe selected (up to 7 days.)

This value is based on the same threat data as the Talos Disposition value in the Incident Promotion Reason tile, but the counts may differ because of the way they are calculated. For example, Talos IP Reputation counts source and destination IP addresses separately, while the Talos Disposition value increments only once per incident, even if both source and destination IP addresses have poor reputation.

The Talos IP Reputation threat metric used to promote events from SSE to incidents is not used in FTD devices. It is similar to, but different from, the Security Intelligence data for networks.

You can view event details in Security Services Exchange (SSE) by clicking a metric in this tile. SSE will open in a separate browser window.

The count of events shown in SSE may differ from the count of events shown in the tile. Duplicate events are automatically removed from SSE, and your configurations in SSE may automatically filter out events. The SecureX tile shows the event count before such actions are taken in SSE.

### Intrusion Top Attackers Tile

List of top attackers for intrusion events in your organization that were sent from FTD devices to SSE.

This tile shows up to 7 days worth of data, even if a longer timeframe is selected at the top of the dashboard. Look at the timeframe selected on the tile itself.

### Intrusion Top Targets Tile

List of top targets for intrusion events in your organization that were sent from FTD devices to SSE.

This tile shows a maximum of 7 days worth of data, even if a longer timeframe is selected at the top of the dashboard. Look at the timeframe selected on the tile itself.

### Intrusion Top Signatures Tile

List of top signatures for intrusion events in your organization that were sent from FTD devices to SSE.

This tile shows a maximum of 7 days worth of data, even if a longer timeframe is selected at the top of the dashboard. Look at the timeframe selected on the tile itself.

### Device Inventory Tile




---

**Important** In order to use this tile, Cisco Success Network must be enabled in each FMC. Enable this feature on the System > Smart Licenses page in FMC. If you have questions, search the FMC online help for "Cisco Success Network".

---

This tile shows only data from deployments with FMC. Devices managed by FDM are not reflected in this tile.

This tile shows whether the FMC appliances that are registered to SecureX, and their managed devices, are running at least the suggested software version. This minimum version may not be the latest available software version. Instead, it is determined by Cisco based on software quality, stability, and longevity.

For best protection, all of your FMCs and all managed devices should be running at least the suggested version. For upgrade instructions, see the *Cisco Firepower Management Center Upgrade Guide* at <https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-guides-list.html>.

Clicking the **Suggested version** link takes you to the Software Downloads page on Cisco.com for Virtual Appliance downloads. The same download can be used for all virtual and hardware FMC appliances.

A zero (0) in the **Managed devices needing upgrade** column indicates that all of this FMC's managed devices are up to date.

### Security Update Status Tile




---

**Important** In order to use this tile, Cisco Success Network must be enabled in each FMC. Enable this feature on the System > Smart Licenses page in FMC. If you have questions, search the FMC online help for "Cisco Success Network".

---

This tile shows only data from deployments with FMC. Devices managed by FDM are not reflected in this tile.

For effective protection, your system should always use the latest threat intelligence.

If this tile shows that your deployment is not up to date, download and install the latest updates.

For information about these updates and options and instructions for manually or automatically installing them, see the "System Updates" chapter in your FMC online help.

### Security Capabilities Tile



**Important** In order to use this tile, Cisco Success Network must be enabled in each FMC. Enable this feature on the System > Smart Licenses page in FMC. If you have questions, search the FMC online help for "Cisco Success Network".

This tile shows only data from deployments with FMC. Devices managed by FDM are not reflected in this tile.

This tile indicates how extensively you are using the security features. Specifically:

- The number of devices managed by each FMC that have been assigned each type of license.
- The number of rules that require each type of license that have been deployed to any device managed by each FMC.

As a simple example, if you have 1 access control policy that has 3 URL filtering rules, and you have deployed that policy to 4 managed devices, the rule count is 12.

### Troubleshooting

If you don't see an answer to your problem in this document, see the *Cisco Firepower and SecureX Integration Guide*, available at <https://cisco.com/go/firepower-securex-documentation>.

## Orbital

Tile Name	Description
User Query and Results Stats	A set of metrics describing user queries and results.
Organization Query and Results Stats	A set of metrics describing organization queries and results.
User Catalog Stats	A set of metrics describing the most highly used catalog queries for this user.
Organization Catalog Stats	A set of metrics describing the most highly used catalog queries for this organization.

## Secure Client

Tile Name	Description
Computer Summary	Shows the number of computers and their issues such as those with conflicting instance key, no instance key, failed package install, failed package reconfigure, and without identity.
Unified Connector Stats	Shows the number of unified connectors and their stats such as those with conflicting keys, without key, install failures, reconfigure failures, and without identity.

## Secure Cloud Analytics

Secure Cloud Analytics (formerly Stealthwatch Cloud) is a software as a service (SaaS) solution that monitors your on-premises and cloud-based network deployments. By gathering information about your network traffic, it creates observations about the traffic, which are facts about behavior on the network, and automatically identifies roles for network entities based on their traffic patterns. Observations on their own do not carry meaning beyond the fact of what they represent. Based on the combination of observations, roles, and other threat intelligence, Secure Cloud Analytics generates alerts, which are actionable items that represent possible malicious behavior as identified by the system.

Secure Cloud Analytics also identifies observations of interesting behavior (highlighted observations), which you can review from its portal UI. Though these observations do not signify malicious behavior on their own, they may represent otherwise notable traffic on your network.

The following describes the Secure Cloud Analytics tiles that you can display in SecureX, which represent Secure Cloud Analytics findings.

Tile Name	Description
Alert Overview Chart	<p>Displays a multilevel pie chart that shows, based on the selected time frame, in the outer ring:</p> <ul style="list-style-type: none"> <li>• new Secure Cloud Analytics alerts created within the time frame</li> <li>• open Secure Cloud Analytics alerts created before the time frame, and not yet closed within the time frame</li> <li>• closed Secure Cloud Analytics alerts closed during the time frame</li> </ul> <p>And in the inner ring:</p> <ul style="list-style-type: none"> <li>• assigned Secure Cloud Analytics alerts</li> <li>• unassigned Secure Cloud Analytics alerts</li> </ul>

Tile Name	Description
Alert Quick View	Displays the current number of open Stealthwatch Cloud alerts and unassigned Stealthwatch Cloud alerts.
Device Count Chart	Displays the number of unique entities that Stealthwatch Cloud detected transmitting traffic on your network during a given time frame, displayed as a vertical bar chart.
Observation Count	Displays the total number of observations that Stealthwatch Cloud generated in a given time frame, and the total number of highlighted observations in that time frame. The Observations and Highlighted Observations links take you to the Stealthwatch Cloud portal UI to view more information about these observations.
Sensor Status	Displays a list of your configured Stealthwatch Cloud sensors, and if they are active or inactive.
Traffic Over Time Chart	Displays the amount of inbound traffic, inbound encrypted traffic, outbound traffic, and outbound encrypted traffic monitored by Stealthwatch Cloud for the selected time frame as a stacked bar chart.

## Secure Email Appliance

### Incoming Email Metrics

Tile Name	Description
Incoming Files Handled by Secure Endpoint	A set of metrics summarizing Secure Endpoint analysis of incoming email.
Incoming Mail Summary	A set of metrics summarizing mail flow activity.
Incoming Threat Messages Summary	A set of metrics summarizing threat activity.
Email Summary	A set of metrics summarizing mail flow activity.
Top Incoming Mail Connections by Country	A set of metrics summarizing top incoming mail connections by country.
Top Senders (Domains) by Total Incoming Threat Messages	A set of metrics summarizing top senders (domains) by total incoming threat messages.
Top Senders (IP Addresses) by Total Incoming Threat Messages	A set of metrics summarizing top senders (IP addresses) by total incoming threat messages.

Tile Name	Description
Top Incoming Virus Types Detected	A set of metrics summarizing top incoming virus types detected.
Top URL Spam Messages	A set of metrics summarizing top URL spam messages.

### Outgoing Email Metrics

Tile Name	Description
Outgoing Mail Summary	A set of metrics summarizing outgoing mail flow activity.
Top Outgoing Sender Domains by Total Outgoing Threat Messages	A set of metrics summarizing top sender domains by total outgoing threat messages.
Top Sender IP Addresses by Total Outgoing Threat Messages	A set of metrics summarizing top sender IP addresses by total outgoing threat messages.

## Secure Endpoint

Tile Name	Description
Compromises detected	A set of metrics summarizing compromises detected by AMP.
Computers Summary	A set of metrics summarizing the state of AMP computers.
Summary	A set of metrics summarizing AMP detection and response.
Quarantines	A set of metrics summarizing AMP quarantines by time.
MITRE ATT&CK Tactics detected	A set of metrics summarizing MITRE ATT&CK tactics detected by AMP.
Threat Hunting	Threat hunting incidents by the threat hunting source.
Top Endpoint Compromises	Top compromises by severity score.
Top Dynamic Threats	Top dynamic threats.
Top Malware Threats	Top threats by compromise detections aggregated by detection name.
Top Compromise Observables	Top compromise observables.



## Secure Malware Analytics

Tile Name	Description
Threat Scores	Counting submissions by threat score ranges.
Total Submissions by Result	Counting submissions by status.
Total Submissions by Threat Score	Counting submissions by threat score ranges.
Total Convictions	Counting total convicted submissions.
Submissions Source by Result	Counting submissions by status, grouped by submission source.
Submission Source by Threat Score	Counting submissions by threat score ranges, grouped by submission source.
Submission Environments	Counting convicted vs. non-convicted submissions, grouped by environment.
Submission File Types	Counting submissions by file type.
Entitlement API Sample Submissions	Counting submissions vs. rate-limited submissions.
Submission Network Exits	Counting submissions by the network exit used during analysis.
Top Tags	Counting submissions by tag.
Top IP Addresses	Counting submissions by IP referenced during analysis.
Top Domains	Counting submissions by domain referenced during analysis.
Top Behavioral Indicators	Counting indicators triggered during submissions.

## Secure Network Analytics

Tile Name	Description
Alarming Hosts by Category	Number of hosts in the alarm categories since the last reset hour.
Network Visibility	Statistics for the number of hosts and the amount of traffic.
Top Alarming Hosts	Top 7 inside hosts, sorted by alarm severity, that have been active on your network since the last reset hour.

Tile Name	Description
Top Alarms By Count	Top 10 alarms by count.
Top Inside Host Groups by Traffic	Top 10 inside host groups by traffic.
Top Outside Host Groups by Traffic	Top 10 outside host groups by traffic.
Visibility Assessment	Number of hosts in the Visibility Assessment categories.

## Secure Web Appliance

Tile Name	Description
Incoming Filed Analyzed by AMP	A set of metrics summarizing incoming files analyzed by AMP.
HTTPS Reports	A set of metrics summarizing web transactions for HTTP and HTTPS traffic.
Top Domains	A set of metrics summarizing top domains in web transactions.
Top Malware Categories	A set of metrics summarizing top malware categories in web transactions.
Top URL Categories	A set of metrics summarizing top URL categories in web transactions.

## SecureX Threat Response

Tile Name	Description
Incident Statuses and Assignees	Displays incidents that are assigned to the current logged in user and others, based on the incident status. Using this tile, you can quickly see incident status and assignees.
High Impact Incidents	Displays the top compromises known to Incident Manager. These incidents are those shown in the High Impact list in SecureX Threat Response Incident Manager or the Incidents app in the SecureX ribbon.

## Security Management Appliance (Email)

### Incoming Email Metrics

Tile Name	Description
Incoming Files Handled by Secure Endpoint	A set of metrics summarizing Secure Endpoint analysis of incoming email.
Incoming Mail Summary	A set of metrics summarizing mail flow activity.
Incoming Threat Messages Summary	A set of metrics summarizing threat activity.
Email Summary	A set of metrics summarizing mail flow activity.
Top Incoming Mail Connections by Country	A set of metrics summarizing top incoming mail connections by country.
Top Senders (Domains) by Total Incoming Threat Messages	A set of metrics summarizing top senders (domains) by total incoming threat messages.
Top Senders (IP Addresses) by Total Incoming Threat Messages	A set of metrics summarizing top senders (IP addresses) by total incoming threat messages.
Top Incoming Virus Types Detected	A set of metrics summarizing top incoming virus types detected.
Top URL Spam Messages	A set of metrics summarizing top URL spam messages.

### Outgoing Email Metrics

Tile Name	Description
Outgoing Mail Summary	A set of metrics summarizing outgoing mail flow activity.
Top Outgoing Sender Domains by Total Outgoing Threat Messages	A set of metrics summarizing top sender domains by total outgoing threat messages.
Top Sender IP Addresses by Total Outgoing Threat Messages	A set of metrics summarizing top sender IP addresses by total outgoing threat messages.

## Security Management Appliance (Web)

Tile Name	Description
HTTPS Reports	A set of metrics summarizing web transactions for HTTP and HTTPS traffic.

Tile Name	Description
Incoming Files Analyzed by Secure Endpoint	A set of metrics summarizing incoming files analyzed by Secure Endpoint.
Top Domains	A set of metrics summarizing top domains in web transactions.
Top Malware Categories	A set of metrics summarizing top malware categories in web transactions.
Top URL Categories	A set of metrics summarizing top URL categories in web transactions.

## Tetration

Tile Name	Description
Tetration Monitored Inventory Metrics	Metrics describing the current learned inventory.
Tetration Policy Metrics	Metrics describing the configured segmentation policies.
Tetration Software Agents Summary	Metrics describing the connected software agents.

## Umbrella

Tile Name	Description
Security Blocks by Command-and-Control Category	A set of metrics summarizing security blocks by command-and-control category.
Security Blocks by Cryptomining Category	A set of metrics summarizing security blocks by the cryptomining category.
Security Blocks by Malware Category	A set of metrics summarizing security blocks by malware category.
Security Blocks by Phishing Category	A set of metrics summarizing security blocks by phishing category.
Cloud Malware Summary	A set of metrics summarizing Cloud Malware for approved applications.
Request Summary	A set of metrics summarizing Umbrella Requests.
Firewall Sessions and Blocks	Total firewall sessions and blocks.
Proxy Sessions and Blocks	Total proxy sessions and blocks.

Tile Name	Description
Proxy Security Blocks	Total proxy security blocks.

## History for SecureX Tiles List

Product(s)	Date of Change	Tile(s)	Description
Secure Client	10/13/2022	Computer Summary, Unified Connector Stats	Added these two new tiles.
Secure Malware Analytics	10/13/2022	Top Behavioral Indicators	Added this one new tile.
Orbital	10/13/2022	User Query and Results Stats, Organization Query and Results Stats, User Catalog Stats, Organization Catalog Stats	Updated the tile names and descriptions.
Duo	10/13/2022	Duo Trust Monitor	Added the new Duo integration module with its one new tile.
Cisco Defense Orchestrator	10/13/2022	CDO VPN, CSDAC Elements, CSDAC Source Connectors, CSDAC Destination Adapters, CSDAC Dynamic Objects	Added these five new tiles.
Umbrella	10/13/2022	Firewall Sessions and Blocks, Proxy Sessions and Blocks, Proxy Security Blocks	Added these three new tiles.
Secure Endpoint	10/13/2022	Top Dynamic Threats	Added this one new tile.

Product(s)	Date of Change	Tile(s)	Description
Cloud Mailbox	03/25/2022	Messages by Direction, Malicious & Phishing, Spam, Graymail	Added the new Cloud Mailbox integration module with its four new tiles.
Orbital, SecureX Threat Response, Secure Malware Analytics	03/10/2022	—	Updated the tiles for Secure Malware Analytics and Orbital; added a new topic for SecureX Threat Response tiles.
Firepower	03/03/2021	Security Update Status	A new Security Update Status tile shows whether your system is using the latest threat intelligence to protect your network.
Firepower	03/03/2021	Security Capabilities	A new Security Capabilities tile summarizes the security features that your system is using, as indicated by the number of licenses and the number of rules in use.
Firepower	03/03/2021	Device Inventory	A new Device Inventory tile summarizes the appliances and devices that you should upgrade.
Firepower	07/23/2020	Raw Event Summary	<p>This tile is now the Event Summary tile.</p> <p>The previous description was:</p> <p>This tile summarizes all events sent to SSE within the timeframe selected, up to 7 days.</p> <p>The count of events shown in SSE may differ from the count of events shown in the tile. Duplicate events are automatically removed from SSE, and your configurations in SSE may automatically filter out events. The SecureX tile shows the event count before such actions are taken in SSE.</p>

