Cisco Secure Network Analytics

Customer Success Metrics Configuration Guide 7.4.2

Table of Contents

Overview **3**

Configuring the Network Firewall **4**

Configuring the Manager 4

Disabling Customer Success Metrics **5**

Customer Success Metrics Data **6**

Collection Types 6

Metrics Details 6

Flow Collector 7

Flow Collector StatsD 10

Manager 12

Manager StatsD 15

UDP Director 20

All Appliances 20

Contacting Support **22**

Change History **23**

Overview

Customer Success Metrics enables Cisco Secure Network Analytics (formerly Stealthwatch) data to be sent to the cloud so that we can access vital information regarding the deployment, health, performance, and usage of your system.

- **Enabled:** Customer Success Metrics is automatically enabled on your Secure Network Analytics appliances.
- **Internet Access:** Internet access is required for Customer Success Metrics.
- **Cisco Security Service Exchange:** Cisco Security Service Exchange is enabled automatically in v7.4.x and is required for Customer Success Metrics.
- **Data Files:** Secure Network Analytics generates a JSON file with the metrics data. The data is deleted from the appliance immediately after it is sent to the cloud.

This guide includes the following information:

- **Configuring the Firewall:** Configure your network firewall to allow communication from your appliances to the cloud. Refer to **Configuring the Network Firewall**.
- **Disabling Customer Success Metrics:** To opt out of Customer Success Metrics, refer to **Disabling Customer Success Metrics**.
- **Customer Success Metrics:** For details about the metrics, refer to **Customer Success Metrics Data**.

> For assistance, please contact Cisco Support.

Configuring the Network Firewall

To allow communication from your appliances to the cloud, configure your network firewall on your Cisco Secure Network Analytics Manager (formerly Stealthwatch Management Console).

> Make sure your appliances have Internet access.

Configuring the Manager

Configure your network firewall to allow communication from your Managers to the following IP addresses and port 443:

- api-sse.cisco.com
- est.sco.cisco.com
- mx*.sse.itd.cisco.com
- dex.sse.itd.cisco.com
- eventing-ingest.sse.itd.cisco.com

> If public DNS is not allowed, make sure you configure the resolution locally on your Managers.

Disabling Customer Success Metrics

Use the following instructions to disable Customer Success Metrics on an appliance.

1. Log in to your Manager.
2. Select **Configure** > **GLOBAL Central Management**.
3. Click the ••• (**Ellipsis**) icon for the appliance. Choose **Edit Appliance Configuration**.
4. Click the **General** tab.
5. Scroll to the **External Services** section.
6. Uncheck the **Enable Customer Success Metrics** check box.
7. Click **Apply Settings**.
8. Follow the on-screen prompts to save your changes.
9. On the Central Management Inventory tab, confirm the Appliance Status returns to **Connected**.
10. To disable Customer Success Metrics on another appliance, repeat steps 3 through 9.

Customer Success Metrics Data

When Customer Success Metrics is enabled, the metrics are collected in the system and uploaded every 24 hours to the cloud. The data is deleted from the appliance immediately after it is sent to the cloud.

We do not collect identification data such as host groups, IP addresses, user names, or passwords.

> For information on data retention and how to request deletion of usage metrics collected by Cisco, refer to Cisco Secure Network Analytics Privacy Data Sheet.

Collection Types

Each metric is collected as one of the following collection types:

- **App Start**: One entry every 1 minute (collects all the data since the application started).
- **Cumulative**: One entry for a 24-hour period
- **Interval**: One entry every 5 minutes (total of 288 entries per 24-hour period)
- **Snapshot**: One entry for the point in time the report is generated

> Some of the collection types are collected at different frequencies than the defaults we've described here, or they may be configured (depending on the application). Refer to **Metrics Details** for more information.

Metrics Details

We've listed the collected data by appliance type. Use Ctrl + F to search the tables by keyword.

Flow Collector

Metric Identification	Description	Collection Type
devices_cache.active	Number of active MAC addresses from ISE in the devices cache	Snapshot
devices_ cache.deleted	Number of deleted MAC addresses from ISE in the devices cache because they have timed out	Cumulative
devices_ cache.dropped	Number of dropped MAC addresses from ISE because the devices cache is full	Cumulative
devices_cache.new	Number of new MAC addresses from ISE added into the devices cache	Cumulative
flow_stats.fps	Outbound flows per second in the last minute	Interval
flow_stats.flows	Inbound flows processed	Interval
flow_cache.active	Number of active flows in the Flow Collector flow cache	Snapshot
flow_cache.dropped	Number of flows dropped because the Flow Collector flow cache is full	Cumulative
flow_cache.ended	Number of flows ended in the Flow Collector flow cache	Interval
flow_cache.max	Maximum size of the Flow Collector flow cache	Interval
flow_ cache.percentage	Percent of capacity of the Flow Collector flow cache	Interval
flow_cache.started	Number of flows added to the Flow Collector flow cache	Cumulative
hosts_cache.cached	Number of hosts in the host cache	Interval

Metric Identification	Description	Collection Type
hosts_cache.deleted	Number of hosts deleted in the host cache	Cumulative
hosts_cache.dropped	Number of hosts dropped because the host cache is full	Cumulative
hosts_cache.max	Maximum size of the host cache	Interval
hosts_cache.new	Number of new hosts added into the host cache	Cumulative
hosts_ cache.percentage	Percent of capacity of the host cache	Interval
hosts_ cache.probationary_ deleted	Number of probationary hosts* deleted in the hosts cache *Probationary hosts are hosts that have never been the source of packets and bytes. These hosts are deleted first when clearing up space in the host cache.	Cumulative
interfaces.fps	Outbound number of interface statistics per second exported to Vertica	Interval
security_events_ cache.active	Number of active security events in the security events cache	Snapshot
security_events_ cache.dropped	Number of security events dropped because the security events cache is full	Cumulative
security_events_ cache.ended	Number of ended security events in the security events cache	Cumulative
security_events_ cache.inserted	Number of security events inserted into the database table	Interval
security_events_ cache.max	Maximum size of the security events cache	Interval

Metric Identification	Description	Collection Type
security_events_cache.percentage	Percent of capacity of the security events cache	Interval
security_events_cache.started	Number of started security events in the security events cache	Cumulative
session_cache.active	Number of active sessions from ISE in the session cache	Snapshot
session_cache.deleted	Number of deleted sessions from ISE in the session cache	Cumulative
session_cache.dropped	Number of sessions from ISE dropped because the sessions cache is full	Cumulative
session_cache.new	Number of new sessions from ISE added into the session cache	Cumulative
users_cache.active	Number of active users in the users cache	Snapshot
users_cache.deleted	Number of deleted users in the users cache because they have timed out	Cumulative
users_cache.dropped	Number of users dropped because the users cache is full	Cumulative
users_cache.new	Number of new users in the users cache	Cumulative
reset_hour	Flow Collector reset hour	N/A
vertica_stats.query_duration_sec_max	Maximum query response time	Cumulative
vertica_stats.query_duration_sec_min	Minimum query response time	Cumulative
vertica_stats.query_duration_sec_avg	Average query response time	Cumulative

Metric Identification	Description	Collection Type
exporters.fc_count	Number of exporters per Flow Collector	Interval

Flow Collector StatsD

Metric Identification	Description	Collection Type
netflow	Total NetFlow records from all Netflow exporters. Includes NVM records.	Cumulative cleared daily
fs_netflow	Netflow records received from Flow Sensors only	Cumulative cleared daily
netflow_bytes	Total NetFlow bytes received from any NetFlow exporter. Includes NVM records.	Cumulative cleared daily
fs_netflow_bytes	NetFlow bytes received from Flow Sensors only	Cumulative cleared daily
sflow	sFlow records received from any sFlow exporter	Cumulative cleared daily
sflow_bytes	sFlow bytes received from any sFlow exporter	Cumulative cleared daily
nvm_endpoint	Unique NVM endpoints seen today (before daily reset).	Cumulative cleared daily
nvm_bytes	NVM bytes received (including flow, endpoint, and endpoint_interface records)	Cumulative cleared daily
nvm_netflow	NVM bytes received (including flow, endpoint, and endpoint_interface records)	Cumulative

Metric Identification	Description	Collection Type
		cleared daily
all_sal_event	All Security Analytics and Logging (OnPrem) events received (including Adaptive Security Appliance and non-Adaptive Security Appliance), counted by number of events received	Cumulative cleared daily
all_sal_bytes	All Security Analytics and Logging (OnPrem) events received (including Adaptive Security Appliance and non-Adaptive Security Appliance, counted by number of bytes received	Cumulative cleared daily
ftd_sal_event	Security Analytics and Logging (OnPrem) (non-Adaptive Security Appliance) events received from Firepower Threat Defense/NGIPS devices only	Cumulative cleared daily
ftd_sal_bytes	Security Analytics and Logging (OnPrem) (non-Adaptive Security Appliance) bytes received from Firepower Threat Defense/NGIPS devices only	Cumulative cleared daily
ftd_lina_bytes	Data Plane bytes received from Firepower Threat Defense devices only	Cumulative cleared daily
ftd_lina_event	Data Plane events received from Firepower Threat Defense devices only	Cumulative cleared daily
asa_asa_event	Adaptive Security Appliance events received from Adaptive Security Appliance devices only	Cumulative cleared daily
asa_asa_bytes	ASA bytes received from Adaptive Security Appliance devices only	Cumulative cleared daily

Manager

Metric Identification	Description	Collection Type
report_complete	Name of the report and the run-time in milliseconds (Manager only)	N/A
report_params	Filters used when the Manager queries the FC databases. Data exported per query: • maximum number of rows • include-interface-data flag • fast-query flag • exclude-counts flag • flows direction filters • order-by column • default-columns flag • Time window start date and time • Time window end date and time • Number of device ids criteria • Number of interface ids criteria • Number of IPs criteria • Number of IP ranges criteria • Number of hostgroups criteria • Number of hosts pairs criteria • Whether results are filtered by MAC addresses • Whether results are filtered by TCP/UDP ports • Number of usernames criteria • Whether results are filtered by number of bytes/packets • Whether results are filtered by total	Snapshot Frequency: Per Request

Metric Identification	Description	Collection Type
	number of bytes/packets • Whether results are filtered by URL • Whether results are filtered by protocols • Whether results are filtered by applications ids • Whether results are filtered by process name • Whether results are filtered by process hash • Whether results are filtered by TLS version • Number of ciphers in cipher suite criteria	
domain.integration_ad_count	Number of AD connections	Cumulative
domain.rpe_count	Number of role policies configured	Cumulative
domain.hg_changes_count	Changes to the Host Group configuration	Cumulative
integration_snmp	SNMP agent usage	N/A
integration_cognitive	Global threat alerts (formerly Cognitive Intelligence) integration enabled	N/A
domain.services	Number of services defined	Snapshot
applications_default_count	Number of applications defined	Snapshot
smc_users_count	Number of users in the Web App	Snapshot
login_api_count	Number of API log ins	Cumulative

Metric Identification	Description	Collection Type
login_ui_count	Number of Web App log ins	Cumulative
report_concurrency	Number of reports running concurrently	Cumulative
apicall_ui_count	Number of Manager API calls using the Web App	Cumulative
apicall_api_count	Number of Manager API calls using the API	Cumulative
ctr.enabled	Cisco SecureX threat response(formerly Cisco Threat Response) integration enabled	N/A
ctr.ats_integration_ enabled	Cisco SecureX ribbon enabled	N/A
ctr.alarm_sender_ enabled	Secure Network Analytics alarms to SecureX threat response enabled	N/A
ctr.alarm_sender_ minimal_severity	Minimal severity of alarms sent to SecureX threat response	N/A
ctr.enrichment_ enabled	Enrichment request from SecureX threat response enabled	N/A
ctr.enrichment_limit	Number of top Security Events to be returned to SecureX threat response	Cumulative
ctr.enrichment_period	Time period for Security Events to be returned to SecureX threat response	Cumulative
ctr.number_of_alarms	Number of alarms sent to SecureX threat response	Cumulative
ctr.number_of_ enrichment_requests	Number of enrichment requests received from SecureX threat response	Cumulative
ctr.number_of_refer_ requests	Number of requests for Manager pivot link received from SecureX threat response	Cumulative

Metric Identification	Description	Collection Type
failover_role	Manager primary or secondary failover role in the cluster	N/A
domain.cse_count	Number of custom security events for a domain ID	Snapshot

Manager StatsD

Metric Identification	Description	Collection Type
swrm_is_in_use	Response Management: Value is 1 if Response Management is used. Value is 0 if it is not used.	Snapshot
swrm_rules	Response Management: Number of custom rules	Snapshot
swrm_action_email	Response Management: Number of custom actions of Email type	Snapshot
swrm_action_syslog_message	Response Management: Number of custom actions of Syslog Message type	Snapshot
swrm_action_snmp_trap	Response Management: Number of custom actions of SNMP Trap type	Snapshot
swrm_action_ise_anc	Response Management: Number of custom actions of ISE ANC Policy type	Snapshot
swrm_action_webhook	Response Management: Number of custom actions of Webhook type	Snapshot
swrm_action_ctr	Response Management: Number of custom actions of threat response Incident type	Snapshot
va_ct	Visibility Assessment: Calculated run-time in milliseconds	Snapshot

Metric Identification	Description	Collection Type
va_ce	Visibility Assessment: Number of errors (when calculation crashes)	Snapshot
va_hcs	Visibility Assessment: Host count API response size in bytes (detect excessive response size)	Snapshot
va_ss	Visibility Assessment: Scanners API response size in bytes (detect excessive response size)	Snapshot
va_ses	Visibility Assessment: Security Events API response size in bytes (detect excessive response size)	Snapshot
sal_input_size	Number of entries in the pipeline input queue	Snapshot Frequency: 1 minute
sal_completed_size	Number of entries in the completed batch queue	Snapshot Frequency: 1 minute
sal_flush_time	Amount of time in milliseconds since the last pipeline flush. Available with Security Analytics and Logging (OnPrem) Single-node only.	Snapshot Frequency: 1 minute
sal_batches_ succeeded	Number of batches successfully written to the file. Available with Security Analytics and Logging (OnPrem) Single-node only.	Interval Frequency: 1 minute
sal_batches_ processed	Number of batches that were processed. Available with Security Analytics and Logging (OnPrem) Single-node only.	Interval Frequency: 1 minute
sal_batches_failed	Number of batches that have failed to complete	Interval

Metric Identification	Description	Collection Type
	writing to the file. Available with Security Analytics and Logging (OnPrem) Single-node only.	Frequency: 1 minute
sal_files_moved	Number of files moved to the ready directory. Available with Security Analytics and Logging (OnPrem) Single-node only.	Interval Frequency: 1 minute
sal_files_failed	Number of files that have failed to be moved. Available with Security Analytics and Logging (OnPrem) Single-node only.	Interval Frequency: 1 minute
sal_files_discarded	Number of files discarded due to error. Available with Security Analytics and Logging (OnPrem) Single-node only.	Interval Frequency: 1 minute
sal_rows_written	Number of rows written to the referenced file. Available with Security Analytics and Logging (OnPrem) Single-node only.	Interval Frequency: 1 minute
sal_rows_processed	Number of rows that were processed. Available with Security Analytics and Logging (OnPrem) Single-node only.	Interval Frequency: 1 minute
sal_rows_failed	Number of rows that failed to be written. Available with Security Analytics and Logging (OnPrem) Single-node only.	Interval Frequency: 1 minute
sal_total_batches_ succeeded	Total number of batches successfully written to the file. Available with Security Analytics and Logging (OnPrem) Single-node only.	App Start Frequency: 1 minute
sal_total_batches_ processed	Total number of batches that were processed.	App Start

Metric Identification	Description	Collection Type
	Available with Security Analytics and Logging (OnPrem) Single-node only.	Frequency: 1 minute
sal_total_batches_ failed	Total number of files that have failed to complete writing to the file. Available with Security Analytics and Logging (OnPrem) Single-node only.	App Start Frequency: 1 minute
sal_total_files_moved	Total number of files moved to the ready directory. Available with Security Analytics and Logging (OnPrem) Single-node only.	App Start Frequency: 1 minute
sal_total_files_failed	Total number of files that have failed to be moved. Available with Security Analytics and Logging (OnPrem) Single-node only.	App Start Frequency: 1 minute
sal_total_files_ discarded	Total number of files discarded due to error. Available with Security Analytics and Logging (OnPrem) Single-node only.	App Start Frequency: 1 minute
sal_total_rows_written	Total number of rows written to the referenced file. Available with Security Analytics and Logging (OnPrem) Single-node only.	App Start Frequency: 1 minute
sal_total_rows_ processed	Total number of rows that were processed. Available with Security Analytics and Logging (OnPrem) Single-node only.	App Start Frequency: 1 minute
sal_total_rows_failed	Total number of rows that failed to be written. Available with Security Analytics and Logging (OnPrem) Single-node only.	App Start Frequency: 1 minute

Metric Identification	Description	Collection Type
sal_transformer_ <transformer id>	Number of transformation errors in this transformer. Available with Security Analytics and Logging (OnPrem) Single-node only.	Interval Frequency: 1 minute
sal_bytes_per_event	Average number of bytes per event received	Interval Frequency: 1 minute
sal_bytes_received	Number of bytes received from the UDP server	Interval Frequency: 1 minute
sal_events_received	Number of events received from the UDP server	Interval Frequency: 1 minute
sal_total_events_ received	Total number of events received by the router	App Start
sal_events_dropped	Number of unparsable events dropped	Interval Frequency: 1 minute
sal_total_events_ dropped	Total number of unparsable events dropped	App Start Frequency: 1 minute
sal_events_ignored	Number of ignored/unsupported events	Interval Frequency: 1 minute
sal_total_events_ ignored	Total number of ignored/unsupported events	App Start Frequency: 1 minute

Metric Identification	Description	Collection Type
sal_receive_queue_size	Number of events in the receive queue	Snapshot Frequency: 1 minute
sal_events_per second	Ingest rate (events per second)	Interval Frequency: 1 minute
sal_bytes_per_second	Ingest rate (bytes per second)	Interval Frequency: 1 minute
sna_trustsec_report_runs	Number of daily TrustSec report requests	Cumulative

UDP Director

Metric Identification	Description	Collection Type
sources_count	Number of sources	Snapshot
rules_count	Number of rules	Snapshot
packets_unmatched	Maximum unmatched packets	Snapshot
packets_dropped	Dropped packets eth0	Snapshot

All Appliances

Metric Identification	Description	Collection Type
platform	Hardware platform (ex: Dell 13G, KVM Virtual	N/A

Metric Identification	Description	Collection Type
	Platform)	
serial	Serial number of the appliance	N/A
version	Secure Network Analytics version number (ex: 7.1.0)	N/A
version_build	Build number (ex: 2018.07.16.2249-0)	N/A
version_patch	Patch number	N/A
csm_version	Customer Success Metrics code version (ex: 1.0.24-SNAPSHOT)	N/A
power_supply.status	Manager and Flow Collector power supply statistics	Snapshot
productInstanceName	Smart Licensing product identifier	N/A

Contacting Support

If you need technical support, please do one of the following:

- Contact your local Cisco Partner
- Contact Cisco Support
- To open a case by web: http://www.cisco.com/c/en/us/support/index.html
- To open a case by email: tac@cisco.com
- For phone support: 1-800-553-2447 (U.S.)
- For worldwide support numbers: https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

Change History

Document Version	Published Date	Description
1_0	March 3, 2023	Initial Version.

Copyright Information