



Cisco Secure Network Analytics

Customer Success Metrics Configuration Guide 7.4.1



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
Contacting Support	28

Overview

Customer Success Metrics enables Cisco Secure Network Analytics (formerly Stealthwatch) data to be sent to the cloud so that Customer Success 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. Click the **Global Settings** icon. Choose **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 Appliance Manager Inventory, 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

The following table lists the data collected by Customer Success Metrics:

Metric Identification	Description	Collection Type
collector.collect.duration_s	Duration it took to collect all metrics	Snapshot Freq: Hourly
devices.cache.active	Number of active	Snapshot

Metric Identification	Description	Collection Type
	MAC addresses from ISE in the devices cache	
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.max	Maximum number of MAC addresses from ISE	Interval
devices.cache.new	Number of new MAC addresses from ISE added into the devices cache	Cumulative
events.vertica.day.{event_id}.count	Total number of each type of security event over one day (delayed by one day)	Interval Freq: Daily
flow_stats	Flow statistics per minute exported to Vertica and ZMQ	Interval
flow_stats.fps	Outbound flows per second in the last minute	Interval
flows	Inbound flows processed	Interval
flows.cache.active	Number of active flows in the Flow Collector flow cache	Snapshot
flows.cache.dropped	Number of flows dropped because the Flow Collector flow	Cumulative

Metric Identification	Description	Collection Type
	cache is full	
flows.cache.ended	Number of flows ended in the Flow Collector flow cache	Interval
flows.cache.max	Maximum size of the Flow Collector flow cache	Interval
flows.cache.percent	Percent of capacity of the Flow Collector flow cache	Interval
flows.cache.started	Number of flows added to the Flow Collector flow cache	Cumulative
flows.dropped	Inbound number of flows dropped	Interval
flows.fps	Inbound number of flows per second	Interval
flows.vertica.all.count	Total number of flow in the database	Snapshot Freq: Daily
flows.vertica.all.last_time.min	Approximation of the oldest flow in database	Snapshot Freq: Daily
flows.vertica.hour.client_ip_address.distinct.catch_all.count	Total number of distinct client IPs belonging to the catch-all group (one hour of data sampled)	Interval Freq: Hourly
flows.vertica.hour.client_ip_address.distinct.count	Total number of distinct client IPs (one hour of data sampled)	Interval Freq: Hourly
flows.vertica.hour.count	Total number of flows in one hour (one hour of data sampled)	Interval Freq: Hourly

Metric Identification	Description	Collection Type
flows.vertica.hour.distinct.count	Approximate number and ratio of unique flow (based on the flow id). Ratio in [0,1] (one hour of data sampled).	Interval Freq: Hourly
flows.vertica.hour.* - inside.inside.count - inside.outside.count - outside.inside.count - outside.outside.count	Total number of flows grouped by direction (one hour of data sampled)	Interval Freq: Hourly
flows.vertica.hour.server_ip_address.distinct.catch_all.count	Total number of distinct server IPs belonging to the catch-all group (one hour of data sampled)	Interval Freq: Hourly
flows.vertica.hour.server_ip_address.distinct.count	Total number of distinct server IPs (one hour of data sampled)	Interval Freq: Hourly
flows.vertica.sample.client_ip_address.distinct.catch_all.ratio	Ratio of client IPs belonging to the catch-all group. Ratio in [0,1] (one hour of data sampled)	Interval Freq: Hourly
flows.vertica.sample.distinct.ratio	Approximate number and ratio of unique flow (based on the flow id). Ratio in [0,1] (one hour of data sampled).	Interval Freq: Hourly
flows.vertica.sample.server_ip_address.distinct.catch_all.ratio	Ratio of server IPs belonging to the catch-all group. Ratio in [0,1] (one hour of data sampled)	Interval Freq: Hourly
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.percent	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	Outbound number of interface statistics exported to Vertica	Interval
interfaces.fps	Outbound number of interface statistics per second exported to Vertica	Interval
platform	Hardware platform (ex: Dell 13G, KVM Virtual Platform)	N/A
product	Secure Network Analytics product (ex: Manager, Flow Collector (NetFlow))	N/A

Metric Identification	Description	Collection Type
report.complete	Name of the report and the run-time in milliseconds (Manager only)	N/A
report.filters	<p>Filters used when the Manager queries the FC databases.</p> <p>Data exported per query:</p> <ul style="list-style-type: none"> • 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 	Snapshot Freq: Per Request

Metric Identification	Description	Collection Type
	<ul style="list-style-type: none"> • 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 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 	
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	Cumulative

Metric Identification	Description	Collection Type
	cache	
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
security_events.cache.percent	Percent of capacity of the security events cache	Interval
security_events.cache.started	Number of started security events in the security events cache	Cumulative
serial	Serial number of the appliance	N/A
sessions.cache.active	Number of active sessions from ISE in the session cache	Snapshot
sessions.cache.deleted	Number of deleted sessions from ISE in the session cache	Cumulative
sessions.cache.dropped	Number of sessions from ISE dropped because the sessions cache is full	Cumulative
sessions.cache.max	Maximum size of the sessions cache	Interval
sessions.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

Metric Identification	Description	Collection Type
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.max	Maximum size of the users cache	Interval
users.cache.new	Number of new users in the users cache	Cumulative
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
vertica.health.node.{node_name}.disk.* - used_bytes - free_bytes - used_ratio	Disk current status	Snapshot Freq: Hourly
vertica.health.node.{node_name}.event.{event_severity}	Count events (one hour of data)	Interval Freq: Daily
vertica.health.node.{node_name}.state	Node current state	Snapshot Freq: Hourly
reset.hour	Flow Collector reset hour	N/A
csm.version	Customer Success Metrics code	N/A

Metric Identification	Description	Collection Type
	version (ex: 1.0.24-SNAPSHOT)	
power.{sensorId}.status	Manager and Flow Collector power supply statistics	Snapshot
integration.ad.{domainId}.count	Number AD connections	Cumulative
rpe.{domainId}.count	Number of role policies configured	Cumulative
rp.{domainId}.count	Number of relationship policies configured	Cumulative
sw.app.{appld}	Secure Network Analytics Apps installed on the system	N/A
hostgroups.changes.{domainId}.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
services.{domainId}.count	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
login.ui.count	Number of Web App log ins	Cumulative
report.concurrency	Number of reports running concurrently	Cumulative

Metric Identification	Description	Collection Type
vertica.stats.query.{user}.duration_sec	Query response time by user	Cumulative
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
exporters.fc.count	Number of exporters per Flow Collector	Interval
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
licensing.smart.smartAccount	Smart Licensing account for the Manager	N/A
licensing.smart.virtualAccount	Smart Licensing virtual account for the Manager	N/A
licensing.smart.registrationStatus	Smart Licensing registration status for the Manager	N/A
licensing.smart.productInstance Name	Smart Licensing product identifier	N/A
ctr.ctr_enabled	Cisco SecureX threat response (formerly Cisco Threat Response) integration enabled	N/A

Metric Identification	Description	Collection Type
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
ctr.swe_visibility_app_metrics	Number of data requests to Visibility Assessment SecureX tile	Cumulative
ctr.swe_visibility_app_network_	Number of data requests to	Cumulative

Metric Identification	Description	Collection Type
metrics	Network Visibility SecureX tile	
ctr.swe_alarming_hosts_by_category	Number of data requests to Alarming Hosts By Category SecureX tile	Cumulative
ctr.swe_top_inside_groups_by_traffic	Number of data requests to Top Inside Hosts SecureX tile	Cumulative
ctr.swe_top_outside_groups_by_traffic	Number of data requests to Top Outside Hosts SecureX tile	Cumulative
ctr.swe_top_alarming_hosts	Number of data requests to Top Alarming Hosts SecureX tile	Cumulative
ctr.swe_top_alarms_by_type_overall	Number of data requests to Top Alarms By Count SecureX tile	Cumulative
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	Snapshot

Metric Identification	Description	Collection Type
	of custom actions of ISE ANC Policy type	
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
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
sources_count	UDP Director: Daily > Number of sources	Snapshot
rules_count	UDP Director: Daily > Number of rules	Snapshot

Metric Identification	Description	Collection Type
packets_unmatched	UDP Director: Daily > Maximum unmatched packets	Snapshot
packets_dropped	UDP Director: Daily > Dropped packets eth0	Snapshot
failover_role	Manager primary or secondary failover role in the cluster	N/A
sal_input_size	Number of entries in the pipeline input queue	Snapshot Freq: 1 minute
sal_completed_size	Number of entries in the completed batch queue	Snapshot Freq: 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 Freq: 1 minute
sal_batches_succeeded	Number of batches successfully written to the file. Available with Security Analytics and Logging (OnPrem) Single-node only.	Interval Freq: 1 minute
sal_batches_processed	Number of batches that were processed. Available with Security Analytics and Logging (OnPrem) Single-node only.	Interval Freq: 1 minute

Metric Identification	Description	Collection Type
sal_batches_failed	<p>Number of batches that have failed to complete writing to the file.</p> <p>Available with Security Analytics and Logging (OnPrem) Single-node only.</p>	<p>Interval</p> <p>Freq: 1 minute</p>
sal_files_moved	<p>Number of files moved to the ready directory.</p> <p>Available with Security Analytics and Logging (OnPrem) Single-node only.</p>	<p>Interval</p> <p>Freq: 1 minute</p>
sal_files_failed	<p>Number of files that have failed to be moved.</p> <p>Available with Security Analytics and Logging (OnPrem) Single-node only.</p>	<p>Interval</p> <p>Freq: 1 minute</p>
sal_files_discarded	<p>Number of files discarded due to error.</p> <p>Available with Security Analytics and Logging (OnPrem) Single-node only.</p>	<p>Interval</p> <p>Freq: 1 minute</p>
sal_rows_written	<p>Number of rows written to the referenced file.</p> <p>Available with Security Analytics and Logging (OnPrem) Single-node only.</p>	<p>Interval</p> <p>Freq: 1 minute</p>
sal_rows_processed	<p>Number of rows that were processed.</p> <p>Available with Security Analytics and Logging (OnPrem) Single-</p>	<p>Interval</p> <p>Freq: 1 minute</p>

Metric Identification	Description	Collection Type
	node only.	
sal_rows_failed	<p>Number of rows that failed to be written.</p> <p>Available with Security Analytics and Logging (OnPrem) Single-node only.</p>	<p>Interval</p> <p>Freq: 1 minute</p>
sal_total_batches_succeeded	<p>Total number of batches successfully written to the file.</p> <p>Available with Security Analytics and Logging (OnPrem) Single-node only.</p>	<p>App Start</p> <p>Freq: 1 minute</p>
sal_total_batches_processed	<p>Total number of batches that were processed.</p> <p>Available with Security Analytics and Logging (OnPrem) Single-node only.</p>	<p>App Start</p> <p>Freq: 1 minute</p>
sal_total_batches_failed	<p>Total number of files that have failed to complete writing to the file.</p> <p>Available with Security Analytics and Logging (OnPrem) Single-node only.</p>	<p>App Start</p> <p>Freq: 1 minute</p>
sal_total_files_moved	<p>Total number of files moved to the ready directory.</p> <p>Available with Security Analytics and Logging (OnPrem) Single-node only.</p>	<p>App Start</p> <p>Freq: 1 minute</p>
sal_total_files_failed	<p>Total number of files that have failed to be moved.</p>	<p>App Start</p> <p>Freq:</p>

Metric Identification	Description	Collection Type
	Available with Security Analytics and Logging (OnPrem) Single-node only.	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 Freq: 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 Freq: 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 Freq: 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 Freq: 1 minute
sal_transformer_<transformer id>	Number of transformation errors in this transformer. Available with Security Analytics and Logging (OnPrem) Single-node only.	Interval Freq: 1 minute
sal_bytes_per_event	Average number of bytes per	Interval

Metric Identification	Description	Collection Type
	event received	Freq: 1 minute
sal_bytes_received	Number of bytes received from the UDP server	Interval Freq: 1 minute
sal_events_received	Number of events received from the UDP server	Interval Freq: 1 minute
sal_total_events_received	Total number of events received by the router	App Start
sal_events_dropped	Number of unparseable events dropped	Interval Freq: 1 minute
sal_total_events_dropped	Total number of unparseable events dropped	App Start Freq: 1 minute
sal_events_ignored	Number of ignored/unsupported events	Interval Freq: 1 minute
sal_total_events_ignored	Total number of ignored/unsupported events	App Start Freq: 1 minute
sal_receive_queue_size	Number of events in the receive queue	Snapshot Freq: 1 minute
sal_events_per second	Ingest rate (events per second)	Interval

Metric Identification	Description	Collection Type
		Freq: 1 minute
sal_bytes_per_second	Ingest rate (bytes per second)	Interval Freq: 1 minute
cse.{domain id}.count	Number of custom security events for a domain ID	Snapshot
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_	Cumulative (cleared daily)

Metric Identification	Description	Collection Type
	interface records)	
nvm_netflow	NVM bytes received (including flow, endpoint, and endpoint_ interface records)	Cumulative (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)

Metric Identification	Description	Collection Type
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)
sna_trustsec_report_runs	Number of daily TrustSec report requests	Cumulative

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>

Copyright Information

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

