

Flow Collector sFlow Update Patch for Cisco Secure Network Analytics (formerly Stealthwatch) v7.4.2

This document provides the patch description and installation procedure for the Cisco Secure Network Analytics Flow Collector sFlow appliance v7.4.2.



There are no prerequisites for this patch, but make sure to review the [Before You Begin](#) section before you get started.

Patch Name and Size


- **Name:** We changed the patch name so that it starts with "update" instead of "patch." The name for this rollup is **update-fcsf-ROLLUP20240317-7.4.2-v2-01.swu**.
- **Size:** We increased the size of the patch SWU files. The files may take a longer time to download. Also, follow the instructions in the [Check the Available Disk Space](#) section to confirm you have enough available disk space with the new file sizes.

Patch Description

This patch, update-fcsf-ROLLUP20240317-7.4.2-v2-01.swu, includes fixes for the following issues:

CDETS	Description
CSCWj00351	Syslog shows Null Pointer Exception on the non-Manager appliances when revocation check is enabled
CSCWj13428	Flow Search and Visibility Assessment show unassigned external IPv6 address in a host group
CSCWi92808	Flow Collector fails to process NVM flows when the NVM lists contain more data than the buffer size
CSCWj13214	Flow Collection Trend graph shows inconsistent flows on the Flow Collector
CSCWj35405	Add flow timestamps and duration to debug_custom_events 1 Advanced Setting for Custom Security Events

CDETS	Description
CSCwj33973	Desktop Client flow query fails with an SQL syntax error
CSCwi51110	SNMP crashes due to segfault error

 Previous fixes included in this patch are described in [Previous Fixes](#).

Before You Begin



Make sure you have enough available space on the Manager for all appliance SWU files that you upload to Update Manager. Also, confirm you have enough available space on each individual appliance.

Check the Available Disk Space

Use these instructions to confirm you have enough available disk space:

1. Log in to the Appliance Admin interface.
2. Click **Home**.
3. Locate the **Disk Usage** section.
4. Review the **Available (byte)** column and confirm that you have the required disk space available on the **/lancope/var/** partition.
 - **Requirement:** On each managed appliance, you need at least four times the size of the individual software update file (SWU) available. On the Manager, you need at least four times the size of all appliance SWU files that you upload to Update Manager.
 - **Managed Appliances:** For example, if the Flow Collector SWU file is 6 GB, you need at least 24 GB available on the Flow Collector (/lancope/var) partition (1 SWU file x 6 GB x 4 = 24 GB available).
 - **Manager:** For example, if you upload four SWU files to the Manager that are each 6 GB, you need at least 96 GB available on the /lancope/var partition (4 SWU files x 6 GB x 4 = 96 GB available).

The following table lists the new patch file sizes:

Appliance	File Size
Manager	5.7 GB
Flow Collector NetFlow	2.6 GB

Appliance	File Size
Flow Collector sFlow	2.4 GB
Flow Collector Database	1.9 GB
Flow Sensor	2.7 GB
UDP Director	1.7 GB
Data Store	1.8 GB

Download and Installation

Download

To download the patch update file, complete the following steps:

1. Go to Cisco Software Central, <https://software.cisco.com>.
2. In the Download and Upgrade section, select **Access downloads**.
3. Type **Secure Network Analytics** in the **Select a Product** search box.
4. Choose the appliance model from the drop-down list, then press **Enter**.
5. Under Select a Software Type, choose **Secure Network Analytics Patches**.
6. Choose **7.4.2** from the Latest Releases area to locate the patch.
7. Download the patch update file, update-fcsf-ROLLUP20240317-7.4.2-v2-01.swu, and save it to your preferred location.

Installation

To install the patch update file, complete the following steps:

1. Log in to the Manager.
2. From the main menu, choose **Configure > GLOBAL Central Management**.
3. Click the **Update Manager** tab.
4. On the Update Manager page, click **Upload**, and then open the saved patch update file, update-fcsf-ROLLUP20240317-7.4.2-v2-01.swu.
5. In the **Actions** column, click the **⋮ (Ellipsis)** icon for the appliance, then choose **Install Update**.



The patch restarts the appliance.

Previous Fixes

The following items are previous defect fixes included in this patch:

Rollup 20240207	
CDETS	Description
CSCwi86232	Unable to upgrade the appliances after replacing the appliances identity certificates
CSCwi72707	Fake App Detect does not exclude iCloud, Gmail, and Yahoo from its exclusion logic on Flow Collector
CSCwi66045	Brute Force Login security event doesn't trigger as expected
CSCwi77099	The alt_brute_force_port Advanced Settings should support up to 10 alternate ports
CSCwi57137	The Flow Collector diagnostic pack does not include the templates.xml file
CSCwi84894	Flow statistic information is inaccurate during a flow search
CSCwi88728	The Msg Server terminates abruptly when the Flow Collector engine is shutting down
CSCwi88729	Invalid IPv4 addresses cause the Flow Collector to crash
CSCwi60663	Exporter_interface structure index limits cause the Flow Collector to crash
CSCwi98047	Custom Security Events need multi-level debugging with debug_custom_events to limit logging output
CSCwi98550	Flow Collector doesn't log the number of flow_stats and flow_interface_stats skipped records each day

Rollup 20240110	
CDETS	Description
CSCwi37680	The Data Store retention management drops large data partition when Data Node is in recovery mode

Rollup 20240110	
CDETS	Description
CSCwi40814	Adding a mitigation action fails in the Desktop Client
CSCwh56984	Manager does not support special characters in the users canonical name for LDAP authentication
CSCwi52748	Flow Collector does not detect 0-byte 0-pkt exporter based on the exporter type
CSCwi52815	The lc-geodata package on the Flow Collector is out-of-date
CSCwi55301	Failover: the appliance status remains Config Channel Down on the promoted primary Manager

Rollup 20231122	
CDETS	Description
CSCwi00243	Authentication issues caused by nginx reloading before client.crt is updated in the trust stores
CSCwh96737	Appliances that have not completed First Time Setup have upgrade errors
CSCwh99593	JOIN Inner Memory error displays for the flow queries with interface data
CSCwi00246	IPv6 traffic causes spurious exporters to populate the exporters.xml
CSCwi11432	The Flow Collector doesn't automatically remove stale interfaces for AWS VPC Flow Log and Cisco ISR exports
CSCwi34041	The purge_templates functionality to remove stale exporters on the Flow Collector is not working
CSCwh91492	Frequent changes in the exporter source id can cause a crash in the Flow Collector processing templates

Rollup 20231018

CDETS	Description
CSCwf39480	The /etc/default/ssh file goes back to its default configuration after rebooting the appliance.
CSCwh78969	Add support to NetFlow v9 for 4-byte count and packet count fields and remove DSCP field validation.

Rollup 20230928

CDETS	Description
CSCwf14756	Fixed an issue in the Desktop Client where the associated flows table was not displaying any flow results.
CSCwh48055	Fixed an issue where Flow Collector Advanced Settings 32-bit range checks were not working for out of range values.
CSCwh49173	Fixed the flow inaccuracy in the Flow Collection Trend graph occurring at the daily reset time.
CSCwh29057	Fixed an issue where the Brute Force Login security event was not detected.
CSCwf89883	The regenerating process for unexpired self-signed appliance identity certificates was simplified. For instructions, refer to the SSL/TLS Certificates Guide for Managed Appliances .

Rollup 20230823

CDETS	Description
CSCwf79482	Fixed an issue where the CLI password was not restored when the Central Management and the appliance backup files were restored.
CSCwh18608	Fixed an issue where the Data Store flow search query ignored process_name and process_hash filtering conditions.

Rollup 20230823	
CDETS	Description
CSCwh14466	Fixed an issue where the Database Updates Dropped alarm was not cleared from the Manager.
CSCwh17234	Fixed an issue where, after the Manager restarted, it failed to download Threat Feed updates.
CSCwf99900	Fixed an issue by revising the debug_custom_events Advanced Setting on the Flow Collector for Custom Security Events.
CSCwh08685	Added cse_exec_interval_secs Advanced Setting to the Flow Collector to control the Custom Security Event (CSE) logic execution interval on a flow.
CSCwh35228	Added SubjectKeyIdentifier and AuthorityKeyIdentifier extensions and clientAuth and serverAuth EKUs to Secure Network Analytics self-signed certificates.

Rollup 20230727	
CDETS	Description
CSCwf71770	Fixed an issue where the database disk space alarms were not functioning correctly on the Flow Collector.
CSCwf80644	Fixed an issue where Manager was unable to handle more than 40 certificates in the Trust Store.
CSCwh08506	Fixed an issue where /lancopelinfo/patch wasn't containing the latest installed patch information for the v7.4.2 ROLLUP patches.

Rollup 20230626	
CDETS	Description
CSCwf73341	Enhanced retention management to collect new data and remove older partition data when the database space is low.

Rollup 20230626

CDETS	Description
CSCwf49883	Excluded nonessential files from the Flow Collector engine diagnostic packs.

Rollup 003

CDETS	Description
CSCwh57232	Fixed an issue where the Flow Collector engine crashed when internal packet capture replay was used.

Rollup 002

CDETS	Description
CSCwf08393	Fixed an issue where the Data Store flow queries failed, because of "JOIN Inner did not fit in the memory" error.

Rollup 001

CDETS	Description
CSCwe49107	Fixed an issue where an invalid critical alarm, SMC_DBMAINT_DSTORE_COMMUNICATION_DOWN was raised on the Manager.

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)

