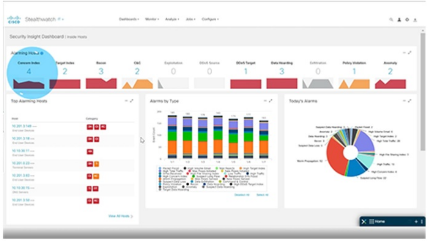
**Manuals+** — User Manuals Simplified.



# CISCO Secure Network Analytics Manager User Guide

Home » Cisco » CISCO Secure Network Analytics Manager User Guide

**Manager 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 Manager (formerly Stealthwatch Management Console) appliance v7.4.2.

ⓘ There are no prerequisites for this patch, but make sure you read Before You Begin section before you get started.

Contents

## 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-smc-ROLLUP20230928-7.4.2-v201.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-smc-ROLLUP20230928-7.4.2-v2-01.swu, includes the following fixes:

| CDETS | Description |
|---|---|
| CSCwe56763 | Fixed an issue where Data Roles could not be created when the Flow Sensor 4240 was set to use Single Cache Mode. |
| CSCwf74520 | Fixed an issue where New Flows Initiated alarm details were 1000 times larger than they should be. |
| CSCwf51558 | Fixed an issue where the Flow Search custom time range filter was not showing results when the language was set to Chinese. |
| CSCwf14756 | Fixed an issue in the Desktop Client where the associated flows table was not displaying any flow results. |
| 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. |

ℹ 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 |
| 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. Log in to Cisco Software Central, **https://software.cisco.com**.
2. In the Download and Upgrade area, choose 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-smc-ROLLUP20230928-7.4.2-v201.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-smc-ROLLUP20230928-7.4.2-v2-01.swu.
5. In the Actions column, click the (Ellipsis) icon for the appliance, then choose Install Update.

ⓘ The patch reboots the appliance.

## Smart Licensing Changes

We have changed the transport configuration requirements for Smart Licensing.

⚠ If you are upgrading the appliance from 7.4.1 or older, make sure that the appliance is able to connect to **smartreceiver.cisco.com**.

## Known Issue: Custom Security Events

When you delete a service, application, or host group, is it is not deleted automatically from your custom security events, which can invalidate your custom security event configuration and cause missing alarms or false alarms. Similarly, if you disable Threat Feed, this removes the host groups Thread Feed added, and you need to update your custom security events.
We recommend the following:

- Reviewing: Use the following instructions to review all custom security events and confirm they are accurate.
- Planning: Before you delete a service, application, or host group, or disable

  Threat Feed, review your custom security events to determine if you need to update them.

  1. Log in to your Manager.
  2. Select Configure > DETECTION Policy Management.
  3. For each custom security event, click the (Ellipsis) icon , and choose Edit.
- Reviewing: If the custom security event is blank or missing rule values, delete the event or edit it to use valid rule values.
- Planning: If the rule value (such as a service or host group) you are planning to delete or disable is included in the custom security event, delete the event or edit it to use a valid rule value.

ℹ For detailed instructions, click the ? (Help) icon.

## Previous Fixes

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

| Rollup 20230823 | |
|---|---|
| CDETS | Description |
| CSCwd86030 | Fixed an issue where Threat Feed Alerts were received after |
| | disabling the Threat Feed (formerly Stealthwatch Threat Intelligence Feed). |
| CSCwf79482 | Fixed an issue where the CLI password was not restored when the Central Management and the appliance backup files were restored. |
| CSCwf67529 | Fixed an issue where the time range was lost and data was not shown when selecting Flow Search Results from a Top Search (with a custom time range selected). |
| CSCwh18608 | Fixed an issue where the  Data Store Flow Search query ignored process_name and process_hash filtering conditions. |
| 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. |
| CSCwh23121 | Disabled unsupported ISE Session Started Observation. |
| 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. |
| CSCwf98685 | Fixed an issue in the Desktop Client where creating a new host group with IP ranges failed. |
| CSCwh08506 | Fixed an issue where /lancope/info/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. |
| CSCwf74281 | Fixed an issue where the queries from hidden elements were causing performance issues in the UI. |
| CSCwh14709 | Updated Azul JRE in the Desktop Client. |

| **Rollup 003** | |
|---|---|
| **CDETS** | **Description** |
| SWD-18734 CSCwd97538 | Fixed an issue where the Host Group Management list was not displayed after restoring a large host_groups.xml file. |
| SWD-19095 CSCwf30957 | Fixed an issue where the protocol data was missing from the exported CSV file, whereas the Port column displayed in UI showed both port and protocol data. |

| **Rollup 002** | |
|---|---|
| **CDETS** | **Description** |
| CSCwd54038 | Fixed an issue where the Filter – Interface Service Traffic dialog box was not shown for filtration when clicking the Filter button on Interface Service Traffic window in the Desktop Client. |

| **Rollup 002** | |
|---|---|
| **CDETS** | **Description** |
| CSCwh57241 | Fixed LDAP timeout issue. |
| CSCwe25788 | Fixed an issue where the Apply Settings button in Central Management was available for unchanged Internet Proxy configuration. |
| CSCwe56763 | Fixed an issue where 5020 error was shown on the Data Roles page when the Flow Sensor 4240 was set to use single Cache Mode. |
| CSCwe67826 | Fixed an issue where the Flow Search filtering by Subject TrustSec was not working. |
| CSCwh14358 | Fixed an issue where the exported CSV Alarms Report had newlines in the Details column. |
| CSCwe91745 | Fixed an issue where the Manager Interface Traffic Report did not show some data when the report was generated for a long period. |
| CSCwf02240 | Fixed an issue preventing Analytics enable and disable when the Data Store password contained whitespace. |
| 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** |
| CSCwe25802 | Fixed an issue where the Manager failed to extract v7.4.2 SWU file. |
| CSCwe30944 | Fixed an issue where the Security Events hopopt was incorrectly mapped to flows. |
| CSCwe49107 | Fixed an issue where an invalid critical alarm, SMC_ DBMAINT_DSTORE_COMMUNICATION_DOWN was raised on the Manager. |

| Rollup 001 | |
|---|---|
| **CDETS** | **Description** |
| CSCwh14697 | Fixed an issue where the Flow Search Results page wasn’t showing the last updated time for a query in progress. |
| CSCwh16578 | Removed the % Complete column from the Finished Jobs table on the Job Management page. |
| CSCwh16584 | Fixed an issue where a Query In Progress message was briefly shown on the Flow Search Results page for completed and canceled queries. |
| CSCwh16588 | Simplified the banner text message on the Flow Search page, Flow Search Results page, and Job Management page. |
| CSCwh17425 | Fixed an issue where Host Group Management IPs were not sorted alpha-numerically. |
| CSCwh17430 | Fixed an issue where the Host Group Management IPs duplication was not eliminated. |

### 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-worldwidecontacts.html**

### Copyright Information

## Documents / Resources

| | |
|---|---|
| | **CISCO Secure Network Analytics Manager** [pdf] User Guide<br>Secure Network Analytics Manager, Network Analytics Manager, Analytics Manager, Manager |

Manager Update Patch for Cisco Secure Network Analytics (formerly Stealthwatch) v7.4.2

### Manager 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 Manager (formerly Stealthwatch Management Console) appliance v7.4.2.

There are no prerequisites for this patch, but make sure you read **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-smc-ROLLUP20230928-7.4.2-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-smc-ROLLUP20230928-7.4.2-v2-01.swu, includes the following fixes:

| CDETS | Description |
|---|---|
| CSCwe56763 | Fixed an issue where Data Roles could not be created when the Flow Sensor 4240 was set to use Single Cache Mode. |
| CSCwf74520 | Fixed an issue where New Flows Initiated alarm details were 1000 times larger than they should be. |
| CSCwf51558 | Fixed an issue where the Flow Search custom time range filter was not showing results when the language was set to Chinese. |
| CSCwf14756 | Fixed an issue in the Desktop Client where the associated flows table was not displaying any flow results. |

© 2023 Cisco Systems, Inc. and/or its affiliates. All rights reserved. - 1 -

## References

- Networking, Cloud, and Cybersecurity Solutions - Cisco
- Support - Cisco Support and Downloads – Documentation, Tools, Cases - Cisco
- Cisco
- Cisco
- Cisco
- Cisco
- Cisco
- Cisco
- Cisco
- Cisco
- Cisco
- Cisco
- Cisco
- Cisco
- Cisco
- Cisco
- Cisco
- Cisco
- Cisco
- Cisco
- Cisco
- Cisco
- Cisco
- Cisco
- Cisco
- Cisco
- Cisco
- Cisco
- Cisco
- Cisco

- Cisco
- Cisco
- Cisco
- Cisco
- Cisco
- User Manual