



# CISCO SWD-14010 Stealthwatch Flow Collector NetFlow User Guide

[Home](#) » [Cisco](#) » CISCO SWD-14010 Stealthwatch Flow Collector NetFlow User Guide 

## Contents

- [1 CISCO SWD-14010 Stealthwatch Flow Collector NetFlow](#)
- [2 Product Information:](#)
- [3 Product Usage Instructions](#)
- [4 Patch Description](#)
- [5 Download and Installation](#)
- [6 Previous Fixes](#)
- [7 Contacting Support](#)
- [8 Copyright Information](#)
- [9 Documents / Resources](#)



## CISCO SWD-14010 Stealthwatch Flow Collector NetFlow



### Product Information:

The Stealthwatch Flow Collector NetFlow Update Patch v7.3.1 is a software update patch for the Stealthwatch Flow Collector NetFlow appliance. This patch, patch-fcnf-ROLLUP008-7.3.1-01.swu, includes several fixes for defects in the previous version.

The patch addresses the following fix:

- Defect SWD-16828: Fixed an issue where Interface Top Reports were showing incorrect results. Rows (all data) were missing when searching for specific hosts or hostgroups, and client or server.

This patch also includes previous defect fixes, which are listed in the user manual.

## Product Usage Instructions

### Download:

1. Go to Cisco Software Central at <https://software.cisco.com>.
2. In the Download and Upgrade section, select "Access downloads".
3. Type "Secure Analytics (Stealthwatch)" in the Select a Product field, then press Enter.
4. Select the appropriate appliance model.
5. Under Select a Software Type, choose "Stealthwatch Patches".
6. Select the desired release version.
7. Download the patch update file, patch-fcnf-ROLLUP008-7.3.1-01.swu, and save it to your preferred location.

### Installation:

1. Log in to the SMC (Stealthwatch Management Console).
2. Click on the Global Settings icon, then click on Central Management.
3. Click on Update Manager.
4. On the Update Manager page, click on Upload, and then open the saved patch update file, patch-fcnf-ROLLUP008-7.3.1-01.swu.
5. Click the Actions menu for the appliance, then click Install Update.

**Note:** The Flow Collector engine will be stopped, and the appliance will be restarted as part of the patch installation process.

#### Stealthwatch Flow Collector NetFlow

##### Update Patch v7.3.1

This document provides a description of the patch and installation procedure for the Stealthwatch Flow Collector NetFlow appliance v7.3.1.

#### Stealthwatch Flow Collector NetFlow Update Patch v7.3.1

This document provides a description of the patch and installation procedure for the Stealthwatch Flow Collector NetFlow appliance v7.3.1.

There are no prerequisites for this patch.

## Patch Description

This patch, patch-fcnf-ROLLUP008-7.3.1-01.swu, includes the following fix:

Defect	Description
SWD-16828	Fixed an issue where Interface Top Reports were showing incorrect results. Rows (all data) were missing when searching for specific hosts or hostgroups, and client or server.

Previous fixes included in this patch are described in a table on the next page.

## **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 Analytics (Stealthwatch) in the Select a Product field, then press Enter.
4. Select the appliance model.
5. Under Select a Software Type, select Stealthwatch Patches.
6. Select All Release, then select release version.
7. Download the patch update file, patch-fcnf-ROLLUP008-7.3.1-01.swu, and save it to your preferred location.

### **Installation**

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

1. Log in to the SMC.
2. Click the Global Settings icon, then click Central Management.
3. Click Update Manager.
4. On the Update Manager page, click Upload, and then open the saved patch update file, patch-fcnf-ROLLUP008-7.3.1-01.swu.
5. Click the Actions menu for the appliance, then click Install Update.

The Flow Collector engine is stopped, and the appliance is restarted as part of the patch installation process.

## **Previous Fixes**

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

Defect	Description
SWD-14010	Fixed an issue with refactor syslog compliance toggling.
SWD-15136	Fixed issue to prevent database backup from canceling.
SWD-15235	Fixed an issue to enable reloading snmpd for configuration changes.
SWD-15421	Fixed an issue with the rotate Chrony log files.
SWD-15443	Fixed issue with add file check before reading SSL files
SWD-15465	Fixed an issue with incorrect patch version on installing multiple SWUs.
SWD-15574	Fixed an issue with the initiator setting on ASA bi-directional flows. (LSQ-5071)
SWD-15592	Fixed the issue where 50% of Traffic Showing was Unknown on the Dashboard.
SWD-15593	Fixed an issue where some applications were not being detected.
SWD-15679	Fixed issue with secret manager being removed after installing the v7.2.1 update patches.
SWD-15712	Fixed an issue where the SE Query provided incorrect data.
SWD-15713	Fixed an issue where the v7.2.1 update patch installation failed due to docker not running.

Defect	Description
SWD-15730	Fixed an issue where the NVM Process Hash and Parent Process Hash were missing in Flow Collector.
SWD-15732	Fixed issue that was preventing osaxsd-server from completing the package upgrade.
SWD-15574	Fixed an issue with setting the initiator on the second half of an ASA bi-flow. (LSQ-5071)
SWD-15744	Fixed an issue where flows without client and server bytes/packets were missing interface information. (LSQ- 5118)
SWD-15779	Fixed an issue where the Palo Alto, AppId/UserId, fields seemed to initiate the Flow Collector Oversubscribed alarm. (LSQ-4919 )
SWD-15842	Fixed an issue with system alarms not clearing.
SWD-15885	Fixed an issue support for ASA bi-flows with bytes = 0 and pkts > 0 and Flow Action needs to be set
SWD-15947	Fixed an issue where TrustSec and user data were missing from active user sessions in new flows after FC reboot or upgrade.
SWD-15984	Fixed an issue where the eta analysis tool was running when generating diag pack. (LSQ-5308)
SWD-16024	Fixed an issue to prevent enabling the datastore advance option in System Config unintentionally.
SWD-16025	Fixed an issue where running a database backup failed. (LSQ- 5358)
SWD-16030	Fixed an issue with the Flow Collector engine indexing the groups array with values greater than, or equal to, 65535.
SWD-16049	Fixed an issue where the swe-detections-worker service on the Flow Collector wasn't registering observations.

Defect	Description
SWD-16054	Fixed a Port Scan Alarm issue where the associated flow table was empty because the client server wasn't following the initiator order. (LSQ-5366)
SWD-16068	Fixed an issue where docker images weren't cleaned up during package upgrade.
SWD-16087/SWD- 16437	Fixed an issue where flow-based Identities were missing on Users report.
SWD-16111/SWD- 16114	Fixed an issue with SIGSEGV in the Threat Feed Update. (LSQ-5437)
SWD-16163	Fixed an error with flow duration values calculated by the Flow Collector engine.
SWD-16183	Fixed an issue where customized applications were not tagging traffic according to DPI definitions. (LSQ-5456)
SWD-16169 / SWD-16210	Fixed an issue where NetFlow data from Checkpoint exporters didn't process properly due to Checkpoint inadvertently using the PEN field. (LSQ-5470)
SWD-16284	Fixed an issue with the range policy_id value.
SWD-16333	Enhanced the Flow Data Lost alarm to set limits longer than the hard-coded, 30-minute threshold. (LSQ-5549)
SWD-16805 Clones: SWD-16783 SWD-16944	Fixed an issue where Flag counters were not accurate on TCP flows. In addition, some non-TCP flows were displaying TCP flag counters.
SWONE-7828	Fixed an issue where the ingest service was falling behind and not catching up.
SWONE-12159	Added TrustSec improvements.
SWONE-14903 / SWONE-18750	Fixed an issue with three memory-related changes to svc-db- ingest.
SWOS-206	Enabled the upgrade process to continue when upgrading

Defect	Description
	osaxsd-server.
SWOS-357	Updated cryptography dependencies to versions built against CiscoSSL.

## Contacting Support

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


- Contact your local Cisco Partner
- Contact Cisco Stealthwatch 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:

## 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)

© 2022 Cisco Systems, Inc. and/or its affiliates. All rights reserved.

## Documents / Resources

	<p><b><a href="#">CISCO SWD-14010 Stealthwatch Flow Collector NetFlow</a></b> [pdf] User Guide SWD-14010 Stealthwatch Flow Collector NetFlow, SWD-14010, Stealthwatch Flow Collector NetFlow, Flow Collector NetFlow, Collector NetFlow, NetFlow</p>
--	--