Manager Update Patch for Cisco Secure Network Analytics (formerly Stealthwatch) v7.5.0

This document provides the patch description and installation procedure for the Cisco Secure Network Analytics Manager (formerly Stealthwatch Management Console) appliance v7.5.0.

> ℹ 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-ROLLUP20240308-7.5.0-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-ROLLUP20240308-7.5.0-v2-01.swu, includes fixes for the following issues:

CDETS	Description
CSCwi78990	After Analytics is enabled, results are incomplete and jobs are failing
CSCwj30325	Database communication across the private network is broken between dual stack 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	5.3 GB
Flow Collector NetFlow	2.5 GB
Flow Collector sFlow	2.1 GB
Flow Collector Database	1.6 GB
Flow Sensor	2.5 GB
UDP Director	1.5 GB
Data Store	1.6 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 **7.5.0** from the Latest Releases area to locate the patch.
7. Download the patch update file, update-smc-ROLLUP20240308-7.5.0-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-smc-ROLLUP20240308-7.5.0-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.

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

Previous Fixes

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

Rollup 20240222	
CDETS	**Description**
CSCwi81154	Audit Log Destination connection issue during IP fallback in Dual-Stack environment
CSCwi37953	Report Builder search results with filters doesn't show data
CSCwi19387	Report Builder Flow Collection Report fails due to NetFlow v1 and v7
CSCwh56984	Manager doesn’t support special characters in the users canonical name for LDAP authentication
CSCwi55301	Failover: the appliance status remains **Config Channel Down** on the promoted primary Manager
CSCwi37680	The Data Store retention management drops large data partition when the Data Node is in recovery mode

Rollup 20240222	
CDETS	**Description**
CSCwi61377	Visibility Assessment application process uses high volume of CPU resources on the Manager
CSCwi69017	Managerdoesn’t support Chinese language when setting email rule or email action from Response Management
CSCwi37950	Manager is unable to upload the SWU file (firmware/patch update file)
CSCwi51110	SNMP crashes due to segfault error
CSCwj06892	Add support for SLAAC on the management interface

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