Cisco Stealthwatch

Report Builder Release Notes 1.4

Table of Contents

Introduction

This document provides general information as well as improvements and bug fixes for all feature and maintenance releases of Stealthwatch Report Builder v1.4. The latest version of Report Builder is v1.4.5.

Overview

Use Stealthwatch Report Builder to create and customize your reports. We've provided templates for building your reports and parameters for defining your search criteria.

The report results are based on your Stealthwatch data and your data role permissions.

Whether you run a report on a routine basis or to investigate an issue, you can review the details by editing the query and/or changing the chart or table view.

For more information about each report, refer to **Report Templates**.

What's New

Report Builder v1.4.5 includes the following fix:

Defect	Description
LVA-2811	Updated Apache Log4J 2 to v2.15.

If you have an earlier version of v1.4.x installed (compatible with Stealthwatch v7.3.2), install Report Builder v1.4.5. Refer to **Downloading the App** and **Installing Report Builder** for instructions.

> ⚠ Do not uninstall your existing Report Builder app. If you uninstall Report Builder, all files associated with it, including your saved reports and temporary files, are deleted.

Before You Begin

Before you install Report Builder, please read this section.

> Report Builder is subject to export control laws and regulations. By downloading Report Builder, you agree that you will not knowingly, without prior written authorization from the competent government authorities, export or re-export (directly or indirectly) Report Builder to any prohibited destination, end user, or for any end use.

Downloading the App

To download Stealthwatch apps, log in to your Cisco Smart Account at https://software.cisco.com or contact your administrator.

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 **Secure Network Analytics Virtual Manager** or **Secure Network Analytics Manager**.
5. Under Select a Software Type, select **App- Report Builder**.
6. Select **All Release**, then select **1.4.5**.
7. Download the app-smc-sw-report-builder-1.4.5.swu, and save it to your preferred location.

App Compatibility with Stealthwatch

When you update Stealthwatch, the app that is currently installed will be retained. However, the app may not be compatible with the new Stealthwatch version. Refer to the Stealthwatch Apps Version Compatibility Matrix to determine which app version is supported by a particular version of Stealthwatch.

You can have only one version of an app installed on your Stealthwatch Management Console (SMC). Use the App Manager page to manage your installed apps. From this page you can install, update, uninstall, or view the status of an app. Refer to the following table to learn about the possible app statuses, and note the following:

- **Check:** Since it is possible that a newer version of an app exists and is not listed in App Manager, always check to see if a newer version is available in Cisco Software Central.
- **Close:** Close Report Builder before you start the update.
- **Install:** Install the newer version over the existing version. You do not need to uninstall your existing app. If you uninstall Report Builder, all files associated with it, including your saved reports and temporary files, are deleted. Do not delete the Report Builder app.

> ⚠ Do not uninstall your existing Report Builder app. If you uninstall Report Builder, all files associated with it, including your saved reports and temporary files, are deleted.

Status	Definition	Actions
UpToDate	Your installed app is the most current version.	No action is required.
UpdateAvailable	You have upgraded to a new version of Stealthwatch. Your existing app is supported by this version of Stealthwatch, but a new version of this app is available.	If you want to update the app, go to Cisco Software Central to download and install the latest version (this will replace your existing version).
UpgradeRequired	You have upgraded to a new version of Stealthwatch, and your existing app is not supported by the Stealthwatch version you are now using.	To continue using this app, go to Cisco Software Central to download and install the latest version (this will replace your existing version).
AppNotSupported	You have upgraded to a new version of Stealthwatch. This app may no longer be supported by the version of Stealthwatch you are now using. It could be that this app has been deprecated or a newer version of this app has not yet been released.	Go to Cisco Software Central to see if a new version has been released.
Error	The installation, upgrade, or removal process for the associated app has not successfully completed.	Contact Cisco Stealthwatch Support. A partial installation, upgrade, or removal of this app may have occurred. If so, this must be corrected.

Resource Usage

Before you install the Report Builder app, confirm you have the required available disk space.

- **Required Available Disk Space:** 600 MB on /lancope/var
- **Details:** Report Builder supports multiple Flow Collectors and domains. The traffic shown in a report represents the data observed in the current domain and all its associated Flow Collectors. Also, keep in mind that this disk space volume is a starting point, and consumption will grow as your system accumulates more data.

To check the available disk space:

1. In the SMC Web App, click the (**Global Settings**) icon.
2. Select **Central Management**.
3. Select the **Appliance Manager** tab.
4. Click the **Actions** menu for the appliance.
5. Select **View Appliance Statistics**.
6. If prompted, log in to the Appliance Administration interface.
7. Scroll to the **Disk Usage** section.
8. Confirm you have the following available disk space: 600 MB on /lancope/var

Failover

When you install the app, it is installed on both the primary and secondary SMCs if you have configured failover. However, the app works only on the primary SMC.

- If the secondary SMC becomes the primary SMC, the app functions on the new primary SMC as if it had been newly installed. No historical data is retained, since no app-related data is transferred between the failover pair.
- If the original primary SMC once again becomes the primary SMC, functionality is restored on this original primary SMC. It retains only the historical data it contained before it became the secondary SMC.
- If the apps or app versions on your primary and secondary SMCs do not match, the apps may not function properly. When there is a mismatch, a message will be displayed prompting you to sync your apps or app versions.

Backup

Refer to the following table to know if Report Builder data and configuration settings can be backed up.

If I perform this type of backup...	Will the associated data be backed up?
Configuration	• Installation is not backed up. • No app-specific configuration is backed up.
Database	• No app-specific data is backed up.

Installing Report Builder

Use the App Manager in Central Management to install Report Builder. We recommend that you use Chrome or Firefox for your browser.

1. Log in to your primary Stealthwatch Management Console.
2. Click the (**Global Settings**) icon.
3. Select **Central Management**.
4. Click the **App Manager** tab.
5. Click **Browse**.
6. Follow the on-screen prompts to upload the app file.
    - **Unavailable:** The Stealthwatch Management Console (SMC) will begin to run immediately after you install it. The page may be unavailable for a few minutes.
    - **Disk Space:** If Stealthwatch has less than 100 MB of disk space, you will not be able to install this app. If the available disk space is between 100 – 600 MB of disk space, you may need to add disk space. For details, refer to **Resource Usage**.
    - **Refresh:** If, while you're working in the app, you begin to switch between Report Builder and the Stealthwatch Web app or other apps, eventually your system will begin to respond more slowly. To resolve this issue, refresh the page.

Opening Report Builder

1. Log in to your primary Stealthwatch Management Console.
2. Select the **Dashboards** menu.
3. Select **Report Builder**.

Online Help

To access the online help for this app, click the (**Help**) icon. The help includes instructions and details about each report.

Report Templates

The following report templates are included in Report Builder.

Name	Description
Alarms Report	Use this report to review a summary of security and Flow Collector alarms. You can investigate alarms for the selected Flow Collector or search across all Flow Collectors.
Data Store Retention Report	Use this report to review the Data Store retention statistics and capacity across all nodes of your Data Store. The Data Store Retention report collects the last 24 hours of data and shows the storage details for various data types and the remaining days of capacity, which is useful for analysis and tuning.
DSCP Status Report	Use this report to review Differentiated Services Code Point (DSCP) status, which is useful for standard network information and reviewing the health of your network. Specifically, you can view traffic, bandwidth, and utilization for a selected interface.
Endpoint Traffic (NVM) Report	Use this report to review endpoint traffic from your Network Visibility Module (NVM). We collect user, device, application, location, and destination data so you can investigate what users are doing while they are on or off the network. **Requirements:** • To receive data on this report, you need Stealthwatch with a Data Store deployment. For information and instructions, refer to the Stealthwatch Data Store Installation and Configuration Guides. • Make sure your Flow Collector is configured to receive data from your Network Visibility

Name	Description
	Module. For instructions, refer to the Endpoint License and NVM Configuration Guide v7.3.2.
Flow Collection Trend Report	Use this report to see the total flow collection data for the Flow Collector and exporter you select. You can use this information to evaluate if a Flow Collector is being over or under-utilized, which is important in capacity planning.
Host Group Application Traffic Report	Use this report to review the application traffic for the host group you select. You can choose to include or exclude applications. This is a good report to monitor data on a daily basis and see a broad overview. If you see a spike in the data, you can focus on the details and determine if there is an issue.
Host Group Flow Traffic Report	Use this report to review host group flow traffic for a selected host group or multiple host groups. Refine your search by including or excluding specific host groups. You can also include or exclude applications, services, and protocols. If you see a spike in the data, focus on the details and determine if there is an issue.
Interface Application Traffic Report	Use this report to review the application traffic for the interface you select.
Interface Service Traffic Report	Use this report to review the service traffic for the interface you select.
NetFlow Collection Status Report	Use this report to check for errors and performance issues on your Flow Collector. You can investigate issues by moving the mouse pointer over the status for each exporter.

Name	Description
Network and Server Performance Report	Use this report to review performance on your Flow Collectors, Flow Sensors, and exporters. For example, if you see that the review round trip time (RTT) is high or increasing, it could indicate latency in the network. **Requirements:** To run this report, you need a Flow Sensor and exporter in your Stealthwatch network with round trip time (RTT) and server response time (SRT) data.
Security Events	Use this report to review a summary of all security events for the time period you select.
System Alarms	Use this report to review a summary of the active system alarms. You can investigate all system alarms or choose specific alarms for your query.
TrustSec Analytics	The TrustSec Analytics report shows the traffic volume between security group tags (SGTs) and details about the application flows between them. Use this report to gain insight into the communication on your network and confirm if your ISE policies are being enforced. **Requirements:** Configure Cisco Identity Services Engine (ISE) with Stealthwatch.
TrustSec Policy Analytics	Use this report to identify possible policy violations, misconfigurations, or deployment issues for the Cisco Identity Services Engine (ISE) egress policy matrix you select. To run this report, you will also select the security group tags (in the report parameters) that you want to investigate. We analyze the flows between security groups to determine if the traffic complies with current policies, which are based on single security group access control lists (SGACL).

Name	Description
	Requirements: Configure Cisco Identity Services Engine (ISE) with Stealthwatch.

Best Practices

To run reports efficiently, review the following:

- **Limit Total Reports/Editing Reports:** Whether you are creating or editing a report, limit the total number of open reports.
- **Time Range Parameter:** If the report template includes custom time ranges, choose short time ranges. This will help maximize performance.
- **Include/Exclude Parameters:** If you select **Include** for a parameter (such as Applications), add at least 1 parameter to the field. Otherwise, the report will search all data in that category, and it will take a long time to run and use a large amount of resources.

App Compatibility Notice

Stealthwatch apps were introduced in v7.0.0 of Cisco Stealthwatch.

Stealthwatch apps are similar in concept to the apps you install on a smartphone. They are optional independently releasable features that enhance and extend the capabilities of Cisco Stealthwatch. You can install, update, and remove Stealthwatch apps using App Manager, which you can access in the SMC Web App under the Central Management menu option.

The release schedule for Stealthwatch apps is independent from the normal Stealthwatch upgrade process. Consequently, we can update Stealthwatch apps as needed without having to link them with a core Stealthwatch release.

To simplify the Stealthwatch customer experience, only one version of a Stealthwatch app will be available to install at any point in time (similar to the app store model). Although we strive for maximum app compatibility, not all versions of an app will be compatible with all versions of Stealthwatch. To learn which app version is supported by a particular version of Stealthwatch, see the Stealthwatch Apps Version Compatibility Matrix.

Some apps may require you to upgrade to the latest version of Cisco Stealthwatch. In addition, when you upgrade your Stealthwatch system, you may need to upgrade some or all of the apps.

Cisco reserves the right to discontinue a Stealthwatch app at any time. There may be many reasons for doing so, including but not limited to the following:

1. The equivalent capabilities provided by the app are now provided elsewhere, either via a new version of the app, a new app, or via a feature in Stealthwatch.
2. The capabilities provided by the app are no longer considered relevant or useful to our customer base.

If the decision is made to discontinue a Stealthwatch app, advance notice will be provided at least sixty days prior to the discontinuation date. Although Stealthwatch apps are currently included with your Cisco Stealthwatch license, Cisco reserves the right to charge license fees for certain Stealthwatch apps in the future.

What's Been Fixed

This section summarizes fixes made in this release. The Stealthwatch story number is provided for reference.

v1.1.5

Defect	Description
SWONE-9882	Running the NetFlow Collection report sometimes returns a 504 Timeout Error.
SWONE-10221	Active Alarm End Time was displayed as 12/31/1969. This has been updated to display "-".
SWONE-10213	Pivot to Flows/Top Reports was not available on the Host Group Flow Traffic report.
SWONE-10322	Active Alarm duration was shown as 00:00:00.xxxx.

v1.1.6

Defect	Description
n/a	

v1.2.1

Defect	Description
n/a	

v1.3.1

Defect	Description
SWONE-13307	Editing a report from the All Reports list could lead to the creation of a new report. Now, if you edit a report, it modifies the appropriate report.
SWONE-10141	Delete was previously unavailable in the menu of a saved report. Now you can delete a report when you have it opened.
SWONE-13187	If you click a report tab, and your session has expired, you will be prompted to log in again.

v1.3.2

Defect	Description
SWAPP-414	In some reports, the link to the Flow Search was broken.
SWAPP-429	We updated the Google Analytics library.
SWAPP-430	Automatic security group tag (SGT) selection in the TrustSec Analytics report was not working properly.
SWAPP-439	Applying a column filter in a report would provide a blank page.
SWONE-13681	In some cases, the TrustSec report results could be shown for 1 day after the start date when the custom date range was used.

v1.3.4

Defect	Description
SWAPP-449	When running the System Alarms report, the Alarm ID column filter was accepting only integer values. Now you can filter by any string.
SWAPP-450	When running the System Alarms report, the System Alarm Type filter entry was not taken into account.
SWAPP-461	After installing Cisco bundles, there was an internal server error that prevented creating new reports.

v1.4.1

Defect	Description
SWAPP-414	Pivot to Flow Search link did not open in Flow Search.
SWONE-8462	Flow Collection Trend report should allow for multiple exporters.

v1.4.4

Defect	Description
SWAPP-439	Applying a column filter in a report would provide a blank page.
SWAPP-447	In the Endpoint Traffic (NVM) report, when using multiple port numbers for the source or destination port filter, the results were not being shown after applying the filter to the total.

Defect	Description
SWAPP-449	When running the System Alarms report, the Alarm ID column filter was accepting only integer values. Now you can filter by any string.
SWAPP-450	When running the System Alarms report, the System Alarm Type filter entry was not taken into account.
SWAPP-461	After installing Cisco bundles, there was an internal server error that prevented creating new reports.

v1.4.5

Defect	Description
LVA-2811	Updated Apache Log4J 2 to v2.15.

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