Cisco Stealthwatch

Release Notes 7.3

Table of Contents

Introduction

Overview

This document provides information on new features and improvements, bug fixes, and known issues for the Stealthwatch v7.3.0 release. For additional information about Stealthwatch, go to cisco.com.

Terminology

This guide uses the term "**appliance**" for any Stealthwatch product, including virtual products such as the Stealthwatch Flow Sensor Virtual Edition (VE).

A "**cluster**" is your group of Stealthwatch appliances that are managed by the Stealthwatch Management Console (SMC). As a subset, a "**Data Store cluster**" is your group of Data Node appliances that comprise your Data Store.

Before You Update

Before you begin the update process, please review the Stealthwatch® Update Guide v7.2.x to v7.3.

Software Version

To update the appliance software to version 7.3, the appliance must have 7.2.1 or later version of 7.2.x installed. It is also important to note the following:

- **Patches:** Make sure you install the latest rollup patch on your appliances before you upgrade. You can download the files from your Cisco Smart Account on Cisco Software Central at https://software.cisco.com.
- **Downloading Files:** Log in to your Cisco Smart Account at https://software.cisco.com or contact your administrator. In the Download and Upgrade section, select **Software Download**. Select **Security** > **Network Visibility and Segmentation** > **Stealthwatch**.
- **Update your appliance software versions incrementally.** For example, if you have Stealthwatch v7.0.x, make sure you update each appliance from v7.0.x to v7.1.x., and then update from 7.1.x to 7.2.x. Each update guide is available on cisco.com.
- **Downgrades:** Version downgrades are not supported because of update changes in data structures and configurations that are required to support new features installed during the update.

- **TLS:** Stealthwatch requires TLS v1.2.
- For increased security, we recommend updating the **IDentity 1000/1100** appliance to v3.3.0.x to take advantage of the new openSSL version with TLS 1.2.

3rd Party Applications

Stealthwatch does *not* support installing 3rd party applications on appliances.

Hardware

To view the supported hardware platforms for each system version, refer to the Hardware and Version Support Matrix.

> ⚠ Dell PowerEdge hardware and the Flow Collector 5020 are *not* supported with Stealthwatch v7.3. For assistance with your hardware refresh, please contact the Stealthwatch Renewals team at stealthwatch_renewals@cisco.com.

Browsers

- **Compatible Browsers:** Stealthwatch supports the latest version of Chrome, Firefox, and Edge.
- **Microsoft Edge:** There may be a file size limitation with Microsoft Edge. We do not recommend using Microsoft Edge to upload the software update files (SWU).
- **Shortcuts:** If you use browser shortcuts to access the Appliance Admin interface for any of your Stealthwatch appliances, the shortcuts may not work after the update process is complete. In this case, delete the shortcuts and recreate them.
- **Certificates:** Some browsers have changed their expiration date requirements for appliance identity certificates. If you cannot access your appliance, log in to the appliance from a different browser, replace the appliance identity certificate with a custom certificate, or contact Cisco Stealthwatch Support.

Alternative Access

Use the following instructions to enable an alternative method to access your Stealthwatch appliances for any future service needs.

> ⚠ It is important to enable an alternative method to access your Stealthwatch appliances for any future service needs, using one of the following methods for your hardware or virtual machine.

Hardware

- **Console (serial connection to console port):** Refer to the latest Stealthwatch Hardware Installation Guide to connect to the appliance using a laptop or a keyboard and monitor. https://www.cisco.com/c/en/us/support/security/stealthwatch/products-installation-guides-list.html
- **CIMC (UCS appliances):** Refer to the latest Cisco guide for your platform at https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/sw/cli/config/guide/b_Cisco_CIMC_CLI_Configuration_Guide/Cisco_CIMC_CLI_Configuration_Guide_chapter1.html

Virtual Appliances

- **Console (serial connection to console port):** Refer to the latest KVM or VMware documentation for your appliance installation.
    - For example, for **KVM**, refer to Virtual Manager documentation.
    - For **VMware**, refer to the vCenter Server Appliance Management Interface documentation for vSphere.

Alternative Method

If you cannot log in to the appliance using the virtual or hardware methods, you can enable SSH on the appliance network interface temporarily.

> ⚠ When SSH is enabled, the system's risk of compromise increases. It is important to enable SSH only when you need it. When you are finished using SSH, disable it.

1. Log in to the Stealthwatch Management Console.
2. Click the **Global Settings** icon.
3. Select **Central Management** .
4. Click **Actions** menu for the appliance.
5. Select **Edit Appliance Configuration**.
6. Select the **Appliance** tab.
7. Locate the **SSH** section.
8. Select whether to enable SSH access only or to also enable root access.

- **Enable SSH:** To allow SSH access on the appliance, check the check box.
- **Enable Root SSH Access:** To allow root access on the appliance, check the check box.

9. Click **Apply Settings**.
10. Follow the on-screen prompts to save your changes.

> ⚠ When SSH is enabled, the system's risk of compromise increases. It is important to enable SSH only when you need it. When you are finished using SSH, disable it.

After You Update

After updating your appliances, please install the required patches:

- patch-smc-ROLLUP001-7.3.0-01.swu or later
- patch-fcnf-ROLLUP001-7.3.0-02.swu or later
- patch-fcsf-ROLLUP001-7.3.0-02.swu or later

Review the patch readme files on Cisco Software Central for details.

What's New

These are the new features and improvements for the Stealthwatch system v7.3 release:

Stealthwatch Data Store

> ⚠ Do **not** deploy a Data Store on your own. Contact Cisco Professional Service for assistance with placement, deployment, and configuration within and as part of your overall Stealthwatch deployment.

The Stealthwatch Data Store provides a central repository to store your network's flow data, collected by your Stealthwatch Flow Collectors. The Data Store provides the following benefits:

- The Data Store provides much greater storage capacity for information collected by your Flow Collectors and overall Stealthwatch deployment.
- The Data Store database is comprised of a cluster of Data Nodes, each containing a portion of your flow data, and a backup of a separate Data Node's data, which provides improved fault tolerance and overall database uptime.
- Because all of your flow data is in one centralized database, as opposed to spread across multiple Flow Collectors, your Stealthwatch Management Console can retrieve query results from the Data Store more quickly than if it queried all of your Flow Collectors separately. Graph and chart population is drastically improved with a Data Store.

Review the Getting Started with the Data Store Guide for more information on Data Store functionality and understand the high-level deployment process. Review the Data Store Cluster Hardware Installation and Configuration Guide for detailed information on deploying a Data Store as part of your Stealthwatch deployment.

Data Store Considerations

If you deploy a Data Store, note the following regarding your Stealthwatch deployment:

- Use the Stealthwatch Web App to monitor and configure your Stealthwatch installation if you deploy a Data Store. The Stealthwatch Desktop Client is incompatible with a Data Store.
- If you configure a Flow Collector for Data Store compatibility, the Appliance Administration interface (Appliance Admin) hides certain functionality. Use Central Management to perform Flow Collector configuration and other related tasks. If

you want to monitor storage statistics, download the Report Builder app to your SMC.

- If you configure your SMC for Data Store compatibility, you cannot use the ETA Cryptographic Audit or Host Classifier apps.
- Endpoint Concentrators are not supported for use with the Data Store.
- Because of the Data Store database architecture, the SMC and all Flow Collectors must communicate with the Data Store, and must be configured during deployment to work with the Data Store. You cannot have a "blended" environment with some Flow Collectors reporting directly to the SMC, and other Flow Collectors reporting to the Data Store.

> If you want to deploy a Data Store to your network, and you already have an SMC 2210 and FC 4210 appliances deployed, you may need to RFD the SMC and Flow Collectors and work with Cisco Professional Services to integrate the Data Store. Contact Cisco Support for more information.

Data Store Architecture

Each Data Store database cluster is comprised of 3 or more Data Nodes. Each Data Node is its own hardware chassis. When you purchase a Data Store, you receive multiple Data Node hardware chassis, corresponding to the number of nodes indicated by that Data Store model. For example, a DS 6200 Data Store provides 3 Data Node hardware chassis. To facilitate inter-Data Node communication as part of the Data Store database cluster, you must deploy 1 or 2 switches that support 10G speeds.

You can purchase more than one Data Store for your deployment. The Data Nodes can be clustered as part of your Data Store database cluster in mulitples of 3, from a minimum of 3 to a maximum of 36.

If you deploy a Data Store with a compatible SMC and Flow Collector, you can configure the SMC and Flow Collector `eth0` management port as an SFP+ fiber port, for increased throughput. Users not deploying a Data Store can only configure the 100 Mbps/1Gbps/10Gbps copper interface as `eth0`.

Review the Stealthwatch Hardware and Software Version Support Matrix for more information on Data Store hardware and Data Store-compatible Stealthwatch appliances.

User Password Validation Requirements and Enhancements

Users will be provided with a suggested password when they click **Generate Password**. Users will have the option to create their own passwords, which must be

between 8 and 256 characters and meet the specific requirements configured in Central Management > Password Policy.

> While entering a password, users now have the option to click **Show Password** to display the characters they're typing.

A user's password cannot:

- be too similar or the same as the user's username,
- have more than four characters the same as their current or previous password,
- contain repeated or sequential characters,
- include a dictionary word of more than four letters,
- or exist on a list of passwords leaked in a data breach.

> These requirements apply to all users, with the exception of the Stealthwatch default Admin.

Response Management

We have moved the Response Management functionality to the Stealthwatch Web App with several improvements, so as of Stealthwatch v7.3.0, you can perform Response Management tasks only in the Stealthwatch Web App. When you upgrade to v7.3.0, Stealthwatch migrates all Response Management configurations from the Stealthwatch Desktop Client to the Stealthwatch Web App. If any migrated rules contain conditions that are incompatible with v7.3.0, Stealthwatch disables them during the migration process. If this occurs, please correct the affected rules before you re-enable them.

When you upgrade from Stealthwatch v7.2 to v7.3, the Stealthwatch Web App imports into Response Management existing Common Event Format (CEF) actions as Syslog Message actions that will use CEF.

When you choose CEF as the format when sending a syslog message, messages now contain the following information:

- Cisco as the Device Vendor
- Stealthwatch as the Device Product
- The current Stealthwatch version as the Device Version

In Stealthwatch v7.3.0, Response Management creates the necessary rules and actions to continue exporting alarms to SecureX Cisco® Threat Response.

We have made the following improvements to Response Management rules and actions:

Rules

- You can specify the exact alarm severity (not only “or higher”).
- Host groups possess multi-selection capability.
- You can select Relationship policies.
- Response Management integrates with Cisco® ISE.
- You have additional predefined rules from which to choose.
- Response Management now includes ISE ANC Policy, Threat Response Incident, and Webhook actions.
- You can easily distinguish custom security events from alarms when choosing them during rule configuration.
- You can more easily add sub conditions and sub condition sets.
- If you want to move a condition to another condition set, you simply drag and drop it to the desired location.
- You can quickly enable and disable rules on the Rules tab (List view).

> The Stealthwatch Web App does not support specifying several IP ranges using the *multiple ranges* format when creating rules.

Actions

We have added the following new actions:

- **ISE ANC Policy** Use this action to direct Cisco® ISE (Identity Services Engine) to apply an ANC (Adaptive Network Control) policy to a source host or target host for which a host alarm has been triggered. In conjunction with this new action, you can now run the ISE ANC Policy Assignments Report. This report enables you to monitor ISE ANC policy assignments that either Response Management or users manually designate.
- **Threat Response Incident** You can export specific alarms to SecureX Cisco® Threat Response based on any condition that a rule provides. You can also configure the incident confidence level and create customized target entities.
- **Webhook** With this action, Stealthwatch provides more response automation and integration opportunities with external systems via web services or REST APIs. Out of the box, Webhook actions can export alarms directly to Splunk HEC (HTTP Event Collector).

We have enhanced the following existing actions:

- **Email** This action can now use SMTP servers with custom ports, authentication, and encryption. You can specify any email address as well as a mailing list for the recipient, and you can preview the email without having to send it.
- **SNMP Trap** We have added newer encryption protocols for v3.
- **Syslog Message** You can specify the hostname as the destination server. This action incorporates CEF format (which was previously offered as a separate action).

Exporters

The Exporter Hybrid Mode is no longer available.

You can now manage and configure your exporters in the Stealthwatch Web App using the **Configure > Exporters** option. You can also now bulk edit multiple exporters at one time (only the Name and SNMP Configuration fields) in the Stealthwatch Web App, up to a maximum of 10. Stealthwatch inserts a blue vertical bar at the beginning of each row that contains edits.

- You cannot bulk edit exporters in a failover SMC.
- You cannot bulk edit custom configurations.
- You must edit any exporters with the following types using your Central Manager:
    - Flow Sensor
    - Virtual Flow Sensor
    - Endpoint Concentrator

Interfaces

You can now manage and configure your interfaces in the Stealthwatch Web App using the **Configure > Exporters** option and then choosing **View Interfaces** from the Actions column for the applicable exporter. You can also now bulk edit multiple interfaces at one time in the Stealthwatch Web App, up to a maximum of 10. You can edit the Name, Description, Inbound Speed, Outbound Speed, Inbound Threshold, Outbound Threshold, and Locked fields. Stealthwatch inserts a blue vertical bar at the beginning of each row that contains edits.

- You cannot bulk edit interfaces in a failover SMC.

Customer Success Metrics

We have changed some configuration settings for telemetry data collection, including the following:

- updated firewall requirements
- added new metrics for the Flow Sensor and UDP Director

For details, please refer to the Stealthwatch Customer Success Metrics Configuration Guide.

Previously, we have collected certain user data when a customer opted in. We collect this data to assist us in improving your customer experience and our products. As of Stealthwatch system v7.2.1, if you do not want this data collected, you must opt out. To opt out, complete the following actions:

1. Log in to Stealthwatch Management Console.
2. Click on the **Global Settings** icon, and then click **Central Management**.
3. From the context menu in the Actions column for the applicable appliance, choose **Edit Appliance Configuration**.
4. Click the **General** tab.
5. Scroll down to the External Services section and uncheck the **Enable Customer Success Metrics** check box.
6. Click **Apply Settings**.

SMC Failover

Use Failover Configuration to establish a failover pair between two Stealthwatch Management Consoles (SMCs) so that one of them serves as a backup console to the other.

In v7.3.0, we moved the configuration menus from the Desktop Client to the Stealthwatch Web App. When you save the failover configuration, the secondary SMC domain configuration is deleted, so make sure you follow the order, requirements, and instructions in the Stealthwatch Failover Configuration Guide.

> ⚠ If your primary SMC goes offline, please note that the SMCs do not swap roles automatically. Make sure you change the SMC roles in the order shown in the Stealthwatch Failover Configuration Guide.

Configuring Failover

The Stealthwatch Failover Configuration Guide includes details that are critical for a successful configuration, including:

- **Certificates:** To set up trust between appliances so they can communicate, make sure you save the correct certificates to the required appliance Trust Stores.

- **Backup Files:** Back up the appliances before you start the failover configuration.
- **Configuration Order:** Configure the secondary SMC before the primary SMC. When you save the failover configuration, the secondary SMC domain configuration is deleted, so make sure you follow the order, requirements, and instructions in the guide.
- **Changing Roles:** If your primary SMC goes offline, make sure you change the SMC roles in the order shown in the guide. The order is critical, and they do not swap roles automatically.
- **Troubleshooting:** Refer to the Stealthwatch Failover Configuration Guide for solutions.

> ⚠ For a successful configuration and operation, follow the instructions in the Stealthwatch Failover Configuration Guide.

Primary and Secondary Roles

As part of the configuration, you will assign a primary SMC and a secondary SMC. When you save the configuration, the following occurs:

- **Primary SMC**: The primary SMC pushes its domain configuration, user settings, and policies to the secondary SMC. Use the primary SMC to manage your appliances, change appliance configurations, change passwords, define alarms, apply policies, and more.
- **Secondary SMC**: The secondary SMC deletes its configuration, so it can synchronize with the primary SMC configuration and settings. Also, the secondary SMC changes to read-only for all users, which means that you will not have access to sections of the secondary SMC and you cannot retrieve files from the secondary SMC.

Cisco Security Services Exchange

We have added the Cisco Security Services Exchange (SSE) to the External Services section. This option is enabled by default and registers your device in the SSE cloud. Smart Licensing is required for automatic registration, or you can manually register on the SecureX configuration page.

> The following integrations require SSE to be enabled:
>
> - Customer Success Metrics
> - SecureX

SecureX Integration Enhancements

We have moved the configuration for sending Stealthwatch Alarms to the Threat Response Private Intelligence store to Response Management. To send alarms to Threat Response as incidents, complete the following steps:

1. Log in to Stealthwatch Management Console.
2. Click on **Configure > Response Management**.
3. Click on the **Actions** tab, then click **Add New Action > Threat Response Incident**.
4. Fill out the form and click **Save**.

For more information, refer to the *Configuring Response Management* help topic and the SecureX Integration Guide.

> If you configured sending Stealthwatch Alarms to CTR in previous Stealthwatch versions, the Threat Response action will be automatically created.

Cognitive Integration Enhancements

To see the full list of monthly enhancements for the Cognitive engine, refer to the Cognitive Release Notes.

Primary Admin

We changed the Master Admin user to Primary Admin.

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: www.cisco.com/en/US/partner/support/tsd_cisco_worldwide_contacts.html

What's Been Fixed

This section summarizes fixes made in this release for issues (bugs/defects) reported by customers in previous releases. The Stealthwatch Defect (SWD or LSQ) number is provided for reference.

Version 7.3.0

Defect	Description
SWD-14260	Updated the code to honor the initiator as the first thing in the client/server setting function. (LSQ-4635)
SWD-14930	Fixed an issue where the Desktop Client was displaying the previous login time in UTC regardless of the user's timezone. (LSQ-4833)
SWD-14932	Fixed an issue where the Cognitive documentation links were out of date.
SWD-14952	Added a warning pop-up to SystemConfig when attempting to change the IP address, if the appliance is managed by Central Management. (LSQ-4380)
SWD-15024	Fixed an issue where the Flow query via API returned a negative value for the tcpConnections field.
SWD-15062	Fixed an issue where Stealthwatch incidents weren't sent to CTR.
SWD-15134	Fixed an issue where the ISE log was flooded with exceptions which prevented normal diagnostics.
SWD-15149	Fixed an issue where the Top Report was not working when the Connection filter was set to"Port/Protocol" and the Subject Orientation filter was set to "Server". (LSQ-4882)
SWD-15218	Fixed an issue where tomcat was not logging to ciscoj.log.
SWD-15293	Updated the LDAP documentation to list the unsupported

Defect	Description
sWD-15294	characters in the bind user name.
SWD-15341	Fixed an issue with proxy passwords not allowing some special characters. (LSQ-4997)
SWD-15360	Updated the Active Directory documentation with the requirement of a identity management device. (LSQ-4991)
SWD-15441	Fixed an issue where the SecureX Top Host Groups By Traffic tiles did not show data.

Known Issues

This section summarizes issues (bugs) that are known to exist in this release. Where possible, workarounds are included. The defect number is provided for reference.

Defect Number	Description	Workaround
SWD-7655	The generation of a diagnostics pack may fail in large systems as a result of timing out.	To overcome this, open the SSH console for the appliance and run this command: doDiagPack. This will allow the generation of the diagnostic pack without timing out. The diagnostic pack can be downloaded using Browse File in the /admin/diagnostics folder, and it can be copied off the box using SCP.
SWD-8197	The Flow Sensor was not detecting enough applications.	To provide more accurate application classification, we updated the third-party library for Application Identification. Due to this update, some traffic will no longer be classified as it was in prior versions and support has been removed for a variety of applications. Updates to the applications supported are dependent on future releases from the third-party library.
SWD-8673	SystemConfig special character fonts look bad when using the SecureCRT client in ANSI mode.	To overcome this, disable ANSI Color when connecting or use a different client to view the SystemConfig script.
SWD-12141	When installing the pre-SWU patch using the	The message might not clear, but it does not block the update.

Defect Number	Description	Workaround
	SMC System Management page, the Update Status may continue to show "Waiting to install."	Check the log to confirm the pre-SWU patch was installed successfully. Make sure you follow the Finalize procedure in the Stealthwatch Update Guide.
SWD-12574	If a user logs in to the command line interface without any failed attempts, the EPOCH date (January 1, 1970) might be shown.	None currently available.
SWD-13089	Changing the appliance IP address, host name, or network domain name may fail.	Before you change an appliance IP address, host name, or network domain name using the Appliance Setup Tool or System Config, review the instructions in Stealthwatch Online Help. You will remove the appliance from Central Management as part of the procedure. Also, confirm the following: • Before you remove the appliance from Central Management, make sure the Appliance Status is shown as Up. • After you remove the appliance from Central Management, the appliance certificates are removed from the SMC automatically. Check the other appliance trust stores

Defect Number	Description	Workaround
		in your cluster. If the appliance identity certificate (of the appliance you are changing) is saved to other appliance trust stores, delete it. • After you change the appliance IP address, host name, or network domain name, use the Appliance Setup Tool to add the appliance to Central Management.
SWD-13154	We've added process improvements to Stealthwatch Flow Collectors as part of this software update. The update may take up to 2 hours to finish. Make sure the Flow Collector update is completed and the appliance status is shown as Up before you update the next appliance in your cluster. **Flow Collector 5000 Series:** Make sure the database update is completed and the appliance status is shown as Up before you start the engine update. Then,	None currently available.

Defect Number	Description	Workaround
	make sure the engine update is completed and the appliance status is shown as Up before you update the next appliance in your cluster.	
SWD-13964	The database restore does not include the encrypted configuration backup.	To overcome this, perform the database restore without restoring the configuration backup by adding `-r` to the doDbRestore command, then manually restore the encrypted backup.
SWD-14039	Restoring the appliance configuration on the Stealthwatch Management Console disables the Threat Intelligence Feed.	1. Open Central Management. 2. Click the SMC > **Actions** menu. 3. Select **Edit Appliance Configuration**. 4. Select the **General** tab. 5. In the External Services section, check the **Enable Threat Intelligence Feed** check box.
SWD-14057	The Packet Capture page is blank in the SMC Appliance Administration.	We've removed Packet Capture from the SMC Appliance Administration. To use an alternative method, select Help > Stealthwatch Online Help, and follow the instructions for the SMC packet capture.
SWD-14187	Browser rejects certificates and prevents	Some browsers have changed

Defect Number	Description	Workaround
	you from accessing appliances.	their expiration date requirements for appliance identity certificates. If you cannot access your appliance, try the following options: • Log in to the appliance from a different browser. • Replace the appliance identity certificate with a custom certificate. For instructions, refer to Central Management > Edit Appliance Configuration > Appliance tab > SSL/TLS Appliance Identity, and select Online Help. • Contact Cisco Stealthwatch Support.
SWD-14800	Stealthwatch Cloud Dashboard redirects to the registration page after upgrading to v7.2.0.	Enter your Steathwatch Cloud credentials when prompted to navigate to the Stealthwatch Cloud Dashboard.
SWD-14815	When performing a Host Search, the Web UI warning for the Flow Aggregation Service is not accurate due to the docker service being removed from the Admin UI.	Wait 15 minutes and try this action again. If the problem persists, please contact Cisco Stealthwatch Support.
SWD-14855	When using Firefox, the Flow Sensor AST may not present Step 6: Add the	Use a different browser. If using Firefox, clear cache and refresh the page.

Defect Number	Description	Workaround
	appliance to Central Management.	
SWD-14860	We do not support Vertica Backup Restore (VBR)	Do not use Vertica to back up or restore. You could permanently lose data.
SWD-14940	DBNode Retention Manager drops partitions during long database backup periods.	We've added procedures to back up your database that include trimming the database and deleting snapshots after the backup. Make sure you follow the instructions in the Stealthwatch® Update Guide v7.1.x to v7.2. For assistance, please contact Cisco Stealthwatch Support.
SWD-15002	Configuration restore fails after RFD.	If you reset an appliance to its factory defaults, you cannot restore the configuration using Central Management. For assistance, please contact Cisco Stealthwatch Support.
SWD-15550	Cisco ISE Release 2.4.0.357 - Cumulative Patch 10+ cannot connect to Stealthwatch v7.3.0 due to updates to the cipher suite library. (LSQ-5068)	This will be fixed in a future ISE patch. We recommend staying on ISE Release 2.4.0.357 - Cumulative Patch 9, upgrading to ISE Release 2.6, or not upgrading to Stealthwatch v7.3.0.
SWD-15570	Typos in Command to Delete Flow Collector Snapshots	The command to delete Flow Collector snapshots as part of the Back up Database

Defect Number	Description	Workaround
		instructions is incorrect in the help and the update guide. Use the following command to delete SMC and Flow Collector database snapshots: `/opt/vertica/bin/vsql -U dbadmin -w lan1cope -c "select remove_database_snapshot ('StealthWatchSnap1');"` Also, make sure you delete the database snapshots on the SMC and the Flow Collector.
SWD-15623	Error retrieving data on SMC/Flow Collector database	The command to delete Flow Collector snapshots as part of the Back up Database instructions is incorrect in the help and the update guide. Use the following command to delete SMC and Flow Collector database snapshots: `/opt/vertica/bin/vsql -U dbadmin -w lan1cope -c "select remove_database_snapshot ('StealthWatchSnap1');"` Also, make sure you delete the database snapshots on the SMC and the Flow Collector.
NA	On the Flow Sensor VE, “Export Application Identification” is off by default.	To enable application identification, this advanced setting will need to be manually selected.

Change Log

Revision	Revision Date	Description
1_0	TBD	Initial version.
2_0	September 8, 2020	• Added After You Update section for required patches. • Added SWD-15570 to Known Issues. • Added GA date.
2_1	September 28, 2020	• Added Primary Admin section to What's New. • Update the User Password Validation Requirements and Enhancements section. • Updated SWD-15570 in Known Issues. • Added SWD-15623 in Known Issues.

Release Support Information

Official General Availability (GA) date for Release 7.3 is Sept. 3, 2020.

For support timeline information regarding general software maintenance support, patches, general maintenance releases, or other information regarding Cisco Stealthwatch Release Support lifecycle, please refer to Cisco Stealthwatch® Software Release Model and Release Support Timeline Product Bulletin.

Copyright Information