# Table of Contents

**Introduction** .................................................................................................................. 5  
Overview ............................................................................................................................... 5  
Terminology ............................................................................................................................ 5  
Before You Update ................................................................................................................. 5  
  Possible insufficient root partition space ................................................................. 5  
  Find the disk usage for an appliance ........................................................................... 6  
Software Version ..................................................................................................................... 6  
Java .................................................................................................................................... 7  
Stealthwatch for Splunk Application .................................................................................. 7  
3rd Party Applications ........................................................................................................... 8  
Hardware ................................................................................................................................. 8  
Browsers ................................................................................................................................ 8  
Alternative Access .................................................................................................................. 8  
  Hardware ............................................................................................................................ 8  
  Virtual Machines .............................................................................................................. 9  
  Additional Option ............................................................................................................. 9  
After You Update .................................................................................................................. 9  
**What's New** .................................................................................................................... 11  
System ................................................................................................................................ 11  
  Flow Collector .................................................................................................................. 11  
Customer Success Metrics ................................................................................................. 11  
Cognitive Analytics Integration Enhancements ............................................................... 11  
  Superforest ....................................................................................................................... 11  
  Service Modeling ............................................................................................................. 11  
Stealthwatch Botnet Classifier ........................................................................................... 12  
Migration to Amazon Web Services (AWS) Cloud .......................................................... 12  
Stealthwatch Cloud Dashboard ............................................................................................ 12
Signing up Steps ................................................................................................. 12
Setting up your account in Stealthwatch ....................................................... 13
Disabling your account .................................................................................. 14
Dashboard Components .................................................................................. 14
  Alerts ............................................................................................................... 14
  Network Activity ............................................................................................ 15
  Highlighted Observation Summary ............................................................... 16
Policy Management .......................................................................................... 17
  Core Policies ................................................................................................ 17
  Relationship Policies ..................................................................................... 19
  Custom Policies (Custom Security Events) .................................................... 19
Host Group Management ................................................................................... 20
User Management ............................................................................................. 21
  When upgrading from v6.10.x to v7.0 ............................................................ 23
  When installing v7.0 Stealthwatch as a fresh install ....................................... 23
App Manager ..................................................................................................... 24
ISE Integration Enhancements .......................................................................... 25
  Changed the process to get pxGrid client certificates .................................... 25
  Integration Options ......................................................................................... 26
  TrustSec Security Group Tags ....................................................................... 26
  Changed Mitigation Actions .......................................................................... 26
  EAP Chaining Sessions Support ..................................................................... 27
  Performance and Scalability ........................................................................... 27
UCS Hardware .................................................................................................... 27
UDP Director ....................................................................................................... 27
Stealthwatch IDentity Appliance ....................................................................... 28
New software update process .......................................................................... 28
Installation and Configuration .......................................................................... 29
Data Storage ....................................................................................................... 29
Appliance Setup Tool .......................................................... 30
Time Zone UTC ...................................................................... 30
USGv6 Certification .............................................................. 30
Central Management ............................................................. 30
Update Manager .................................................................. 31
Certificates and Trust Store ................................................ 31
Stealthwatch Cloud: Early Access ........................................ 32
Installing the Stealthwatch Desktop Client ............................ 32
Install the Desktop Client Using Windows ............................ 33
Change the memory size ..................................................... 33
Install the Desktop Client Using macOS .............................. 34
Change the memory size ..................................................... 35
Contacting support ............................................................ 36
What’s Been Fixed ................................................................ 37
Version 7.0.0 ...................................................................... 37
Known Issues ....................................................................... 46
Reported 6.10.X > 7.0 Upgrade Issues ................................. 53
Release Support Information ............................................... 54
Introduction

Overview

This document provides information on new features and improvements, bug fixes, and known issues for the Stealthwatch System v7.0.0 release. For additional information about the Stealthwatch System, go to the Customer Community.

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).

Most appliances are managed by the SMC. If an appliance is not managed by the SMC, such as an Endpoint Concentrator, it is described as a "stand-alone appliance."

Before You Update

Before you begin the update process, please review the Stealthwatch® Update Guide v6.10.x to v7.0.0.

⚠️ Before upgrading to 7.0.0, save your update log files. Updating to 7.0.0 deletes these log files.

⚠️ Before patching 7.0.0, save your update log files. Each patch deletes the previous log.

Possible insufficient root partition space

Note the following:

- For systems with a 5 GB or a 7.5 GB root partition on the SMC, after upgrading to v7.0.0, your root consumption will be close to or over the optimal range. This may impact your ability to run future updates or install Stealthwatch apps. Critical functions will stop when your system no longer has enough space in the root partition. For information about how to find the disk usage statistics for an appliance, see Find the disk usage for an appliance immediately below.
- If you are attempting to run a patch, you might need to uninstall one or more apps to free up space.

**Find the disk usage for an appliance**

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 down to the Disk Usage section.
8. Review the top row/ and check the percentage in the **Used** column. This root partition data is shown in red if the usage is 75% or more. As the root partition continues to fill up, critical functions may stop. As the usage gets closer to 100%, you may want to consider an appliance refresh. Please contact [Cisco Stealthwatch Support](https://stealthwatch.flexnetoperations.com) for details.

![Disk Usage Table](image)

**Software Version**

To update the appliance software to version 7.x, the appliance must have 6.10.2, 6.10.3, or later version of 6.10.x installed. It is also important to note the following:

- **Patches:** For each software version, install the required rollup patch files and software update files before you start this update. For details, log in to Stealthwatch's Download and License Center at [https://stealthwatch.flexnetoperations.com](https://stealthwatch.flexnetoperations.com).

The following patches are required for this update:

- **6.10.2:** patch-smc-ROLLUP008-6.10.2-01.swu (or later)
- **6.10.4:** patch-common-lc-admin-6.10.4-01.swu (or later)
• **Update your appliance software versions incrementally.** For example, if you have Stealthwatch v6.8.x, make sure you update each appliance update from v6.8.x to 6.9.x, and then from v6.9.x to v6.10.x. Each update guide is available on the Customer Community or 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 v1.1 or later.

• 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.

**Java**

Stealthwatch requires Java version 8 (latest available update) to run the SMC Desktop Client. We do not support Java versions 9, 10, or 11.

Review the following product capabilities to determine if you need to install the Java Runtime Environment:

• **SMC Desktop Client:** maps, customizable dashboards, response management, system alarms, SLIC configuration, SMC failover configuration, license management across a cluster, TACACS and RADIUS configuration, and Stealthwatch domain editing. Install the Java Runtime Environment only for users who require these capabilities. There may be more capabilities than the information shown here.

• **Web User Interface:** Most product capabilities are available through the Web user interface, and the Java Runtime Environment may not be required.

> In some cases, the Azul JRE launcher may be flagged as a virus and quarantined by your antivirus solution. If this happens, it is a false positive.

Please contact your antivirus provider to have them register the Azul JRE launcher executable as a false positive. The antivirus provider should also have the Azul JRE launcher executable placed on their always approve list.

**Stealthwatch for Splunk Application**

If you are updating to Stealthwatch v7.0 and use the Stealthwatch for Splunk application that is offered through the Advanced Services SIEM Integration Service, you need to update Splunk so that it is compatible with Stealthwatch v7.0. Otherwise, you will experience a disruption in functionality. Make sure you update Splunk *before* you update to Stealthwatch v7.0.
To receive instructions on how to update Splunk, please contact your Stealthwatch Advanced Services Engineer.

### 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](#).

### 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.

### 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

- **iDRAC Enterprise (Dell appliances):** Refer to the latest documentation for your platform at [www.dell.com](http://www.dell.com). iDRAC Enterprise requires a license, and iDRAC Express does not allow console access. If you do not have iDRAC Enterprise, direct console or SSH can be used.

**Virtual Machines**

- **Console (serial connection to console port):** Refer to the latest KVM or VMware documentation for your appliance installation.
  - For example, for **KVM**, see the Virtual Manager documentation at [https://virt-manager.org/](https://virt-manager.org/)

**Additional Option**

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

![Warning](https://i.imgur.com/3Q3Q.png)

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 Appliance Admin interface.
   
   SMC: Log in to the SMC. Click the **Global Settings** icon > **Administer Appliance**.

2. Click **Configuration** > **Services**.

3. Check the **Enable SSH** check box to enable SSH.
   
   To allow the root user SSH access, check the **Enable Root SSH Access** check box.

4. Click **Apply**.

**After You Update**

After updating your appliances, please install the required patches:

- patch-smc-ROLLUP013-7.0.0-03.swu
Review the patch readme files on the Stealthwatch Download and License Center for details.
What's New

These are the new features and improvements for the Stealthwatch System v7.0.0 release:

System

Flow Collector

Your Flow Collector now preserves flow and event records that were active during the shutdown and restart processes. Because of this, your Flow Collector may take longer to shut down and restart.

Customer Success Metrics

Customer Success Metrics (CSM) enables Stealthwatch system data to be sent to the cloud so that Customer Success can access vital information regarding the deployment, health, performance, and usage of your system. For more information about what data is sent to the cloud, go to the CSM data sheet.

Cognitive Analytics Integration Enhancements

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

Superforest

CTA can now leverage detections from the analysis of WebFlow telemetry to improve the efficacy of analyzing NetFlow telemetry from Stealthwatch. This is accomplished by the system through correlation of both telemetry types. According to measurements by Cisco, the number of both confirmed and detected threats should increase by approximately 10%.

Service Modeling

Service modeling is now available for internal servers (on-demand for Stealthwatch customers). The internal servers are specified using the host group definitions. By configuring an internal host group to send Stealthwatch flow records, the user adds additional data to be sent to the Cognitive cloud for analysis. Service Modeling focuses on company internal servers (e.g. mail servers, file servers, web servers, authentication servers etc). Analyzing additional traffic from the end users to those servers can improve the visibility of the exposure of data that may have been misused by malware running on
the affected end user devices. Please do not check all the host groups for sending the data. Only check those host groups that represent internal servers.

**Stealthwatch Botnet Classifier**

CTA can now detect botnets on Stealthwatch flows characterized by a uniform anomalous/unknown communication to many external nodes. In combination with other features, the SVM (Support Vector Machine) classifier is trained specifically to provide high generalization.

**Migration to Amazon Web Services (AWS) Cloud**

Cognitive Analytics migrated to the AWS Cloud in August 2018, resulting in the Cognitive URLs and IP addresses changing and some minor differences in the reported incidents. See the [Field Notice](#) for more information.

**Stealthwatch Cloud Dashboard**

The Stealthwatch Cloud Dashboard integrates Stealthwatch Cloud with the SMC Web Application interface. After setting up your cloud environment, you can use this page to view alerts, network activity, and the highlighted observation summary from Stealthwatch Cloud. For more information, go to the Stealthwatch Cloud [website](#).

> Stealthwatch Cloud integration was implemented in v6.10.2.

**Signing up Steps**

You must be an Admin user to sign up for a Stealthwatch Cloud Account.

To sign up for a Stealthwatch Cloud Account, complete the following steps:

1. Click **Sign Me Up** on the Stealthwatch Cloud Dashboard page.
2. Fill out the form, then click **Start My Free Trial**.

3. Once you receive the email with your account information, set up your cloud account including all of the Stealthwatch users you want to use the Cloud Dashboard.

**Setting up your account in Stealthwatch**

To set up your cloud account, complete the following steps:

1. Click **Enter Account Info** on the Stealthwatch Cloud Dashboard.

2. Enter or edit the URL for your account, then click **Save**.

Only Admin users can edit the SWC URL. When setting up your account, do not include any characters after ".com" for the SWC URL. For example, you would change

3. Enter your SWC Username.
4. Enter your SWC API Key. Click Go Get It to go to the Cloud Settings page where your API key is located.
5. Click Save.

You can access the Stealthwatch Cloud Account Setup tool by going to Deploy > Stealthwatch Cloud.

Disabling your account

You must be an Admin user to disable your Stealthwatch Cloud Account.

To disable your cloud account, complete the following steps:

1. Go to Deploy > Stealthwatch Cloud.
2. Delete the SWC URL.
3. Click Save.

Dashboard Components

Alerts

This component displays a summary of the open alerts, sorted by last updated, for your cloud environment. Use the chart to view the following:

- Number of open alerts.
- Alert name, the source, the date last updated, the number of comments, and the assigned user.

From this component you can access the following information:

- Alert details, which provides in-depth information about the alert. To view this information, click on the alert name.
- List of open alerts in your Stealthwatch Cloud Account. To view this information, click Open in the top right of the component.
- List of alerts assigned to you. To view this information, click Assigned To You in the top right of the component.
- Context menu, which provides the option to view the Alerts or Observations associated with the applicable source. To view the context menu, click the ellipsis next to the applicable Source information.
Network Activity

This component displays traffic in bytes and traffic in connections for the last 24 hours. Use the graph to view the following:

- How much data transferred to and from your network.
- How many bidirectional connections (number of hosts) in your network.
- Alerts. Open alerts are designated by a red triangle with an exclamation point (!) on the point in time when the network activity that triggered the alert occurred. Closed alerts are designated by a green circle with a check mark.

From this component you can access the following information:

- Type, date, time, and source of the alert. To view this information, click on the alert tag.
- Alert details, which provides in-depth information about the alert. To view this information, click on the link from the alert tag context menu.
Highlighted Observation Summary

This component displays the highlighted observations summary and quantity for the last seven days. The highlighted observations are not necessarily security threats - just records of activity considered remarkable by Stealthwatch Cloud's models and algorithms. Once combinations of observations represent a security concern, an alert is generated. Click on the observation name to pivot to all observations for that category.

<table>
<thead>
<tr>
<th>NAME</th>
<th>COUNT (LAST 7 DAYS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bad Protocol</td>
<td>35800</td>
</tr>
<tr>
<td>Persistent External Server</td>
<td>26807</td>
</tr>
<tr>
<td>Heartbeat</td>
<td>7053</td>
</tr>
<tr>
<td>Geographic Blacklist</td>
<td>545</td>
</tr>
<tr>
<td>New External Server</td>
<td>289</td>
</tr>
<tr>
<td>New High Throughput Connection</td>
<td>113</td>
</tr>
<tr>
<td>Long Session</td>
<td>0</td>
</tr>
<tr>
<td>Unusual DNS Resolver</td>
<td>0</td>
</tr>
</tbody>
</table>
Policy Management

You can now manage all security event and related alarm policies (core, relationship, custom) in the SMC Web App. (You can access Policy Management from the Configure main menu option.)

Some IP address range formats that are valid entries in the SMC Desktop Client may not be valid entries in the SMC Web App. Conflicting formats entered in the SMC Desktop Client will display in the corresponding SMC Web App element (e.g., Host Group Management, Policy Management, etc.). However, individual conflicts require modification before you can update the given configuration in the SMC Desktop Client. Please refer to online help for valid formats.

Core Policies

The method in which you enable and disable security events in the SMC Web App is different from the way you accomplish this in the SMC Desktop Client. To see the options you can configure for security events, refer to the following image and table.

<table>
<thead>
<tr>
<th>If this option...</th>
<th>Is selected for &quot;When Host is Source,&quot; then this security event will...</th>
<th>Is selected for &quot;When Host is Target,&quot; then this security event will...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off</td>
<td>Not collect index points nor alarm.</td>
<td>Not contribute index points to alarm category events nor alarm.</td>
</tr>
<tr>
<td>Ignore</td>
<td>Not be used. Stealthwatch will ignore the settings configured for this event in this policy (to which</td>
<td>Not be used. Stealthwatch will ignore the settings configured for this event in this policy (to which</td>
</tr>
</tbody>
</table>
If this option... | Is selected for "When Host is Source," then this security event will... | Is selected for "When Host is Target," then this security event will...
---|---|---
the associated host belongs). It will instead use the settings configured for this event in the next policy (in order of precedence) to which the associated host belongs. For example, if the ignored policy is a host policy, Stealthwatch uses the settings configured for this event in the role policy to which the associated host belongs. If no such role policy exists, then Stealthwatch will use the settings configured for this event in the default policy. **Note:** This option does not apply to alarm category events. | the associated host belongs). It will instead use the settings configured for this event in the next policy (in order of precedence) to which the associated host belongs. For example, if the ignored policy is a host policy, Stealthwatch uses the settings configured for this event in the role policy to which the associated host belongs. If no such role policy exists, then Stealthwatch will use the settings configured for this event in the default policy. |  
On | Collect index points but not alarm. | Contribute index points to alarm category events but not generate alarms.  
On + Alarm | Collect index points and generate alarms. | Contribute index points to alarm category events and generate alarms.

You can search for the following types of effective policies:

- All effective policies with a specific host.
- The effective policies associated with a specific host for only one particular security event type.

Effective policies are now designated by the word “Effective” located inside an orange rectangle.
Any core policies you add to either the SMC Web App or SMC Desktop Client will be displayed in both interfaces.

All role or host policies created before v7.0 will retain their mitigation settings, if any have been configured. You can view and update these mitigation settings only in the SMC Desktop Client.

**Relationship Policies**

In the SMC Web App you can create a relationship policy between two host groups without having to create a map. You can still create maps, but only in the SMC Desktop Client. Additionally, relationship policies now trigger relationship alarms on the Security Insight Dashboard.

Any edits you make to a relationship policy in either the SMC Web App or SMC Desktop Client will be reflected in both interfaces.

**Custom Policies (Custom Security Events)**

You can access custom policies (also known as custom security events) from the Configure > Policy Management main menu option. We have enhanced custom policy
functionality, including a new rule builder and additional rule types. You may now configure custom policies to evaluate flow attributes such as byte ratios, services, process name, and more. You can also specify bytes and packets for a defined side of the communication (subject vs. peer). Additionally, flexibility has been improved to allow the use of operators (<, <=, =, >, >=) with specific values.

The encryption TLS/SSL version, as reported by ETA, is now a component of custom policies. You can easily configure custom policies to alarm when your defined encryption standards are not being met within critical, ETA-enabled segments of your network. Enter a given version level and include the appropriate operator to evaluate as a hierarchical list (“none” being the lowest value and “TLS 1.3” the highest).

TLS 1.3 is still in early adoption and has not been completely defined as an implementation footprint by the industry. Therefore, we recommend that you use > and < operators when using TLS 1.3 rather than = (equal sign).

Finally, to help ensure you are configuring logically valid custom policies, a summary sentence is now displayed for each custom policy you define that describes which elements your policy will evaluate. It may be worth reviewing policies in the SMC Web App that were configured prior to v7.0. To see the summary statement for a custom policy that was configured prior to v7.0, you must first edit it. While editing, use the new rules type to help refine these events further. When finished, click **Save**.

**Host Group Management**

You can now manage and configure your host groups in the SMC Web App. Although you can perform the same host management functions here that you can perform in the SMC Desktop Client, some of the ways in which you do so have slightly changed. The only new element is the Description field.
User Management

You can now manage user account data in the SMC Web App. When you add a user to either the SMC Web App or SMC Desktop Client, you can then view that user account in both interfaces. User Management functionality no longer exists in the SMC (Administration) Admin interface.

In the SMC Web App you can now assign data roles to users. They work the same way in the SMC Web App as they currently do in the SMC Desktop Client. They control which domains, host groups, appliances, and devices a user can view (read) and make configurations to (write). Any edits you make to a user’s data role in either the SMC Web App or SMC Desktop Client will be reflected in both interfaces. You can create custom data roles in the SMC Desktop Client. If you do so, they will also be listed in the SMC Web App.
Web roles are new for Stealthwatch v7.0. They control which functionality (e.g., flow search, policy management, network classification, etc.) in a domain or related to a host group, appliance, or device that users can view and/or configure in the SMC Web App. You can assign and view web roles only in the SMC Web App. You cannot create additional web roles.

Desktop client roles, which are assigned in the SMC Web App, are also new for Stealthwatch v7.0. They control which functionality (e.g., flow search, policy management, reports, etc.) in the SMC Desktop Client that users can view and configure. (In the SMC Desktop Client, Stealthwatch refers to desktop client roles as function roles.) Any edits you make to a user’s desktop client role(s) in either the SMC Web App or SMC Desktop Client will be reflected in both interfaces. You can create custom desktop client roles in the SMC Desktop Client.
Refer to the following two tables, depending on your situation, to see the various web roles and desktop client roles you can assign to users.

**When upgrading from v6.10.x to v7.0**

<table>
<thead>
<tr>
<th>If you created the user...</th>
<th>And in v6.10.x the desktop client role was...</th>
<th>Then in v7.0, the desktop client role is...</th>
<th>Then in v7.0, the web role is...</th>
</tr>
</thead>
<tbody>
<tr>
<td>While setting up the appliance (the user is the System Admin)</td>
<td>System Admin</td>
<td>System Admin</td>
<td>Master Admin (by default) *</td>
</tr>
<tr>
<td>In the Appliance Admin interface</td>
<td>Admin privileges</td>
<td>Admin privileges</td>
<td>Master Admin (by default) *</td>
</tr>
<tr>
<td>In the SMC Desktop Client</td>
<td>Any functional role</td>
<td>The same role as it was before upgrade</td>
<td>Analyst (by default) *</td>
</tr>
</tbody>
</table>

* You can change this role in the SMC Web App.

**When installing v7.0 Stealthwatch as a fresh install**

<table>
<thead>
<tr>
<th>If you created the user...</th>
<th>Then in v7.0, the desktop client role is...</th>
<th>The in v7.0, the web role is...</th>
</tr>
</thead>
<tbody>
<tr>
<td>In the SMC Desktop Client</td>
<td>Any functional role</td>
<td>Analyst (by default) *</td>
</tr>
<tr>
<td>In the SMC Web App, and the user is not the Master Admin</td>
<td>Any functional role</td>
<td>Any web role</td>
</tr>
<tr>
<td>In the SMC Web App, and the user is the Master Admin</td>
<td>Admin privileges</td>
<td>Master Admin</td>
</tr>
</tbody>
</table>

* You can change this role in the SMC Web App.
App Manager

App Manager is one of the new features located within Central Manager. Use the App Manager page to manage your installed Stealthwatch apps. From this page you can install, update, uninstall, or view the status of an app (only a Master Admin can install or uninstall an app). When an app is available for a particular Stealthwatch version, it is posted in Flexera.

Stealthwatch standalone apps will be available in the near future.

You can install and upgrade these standalone apps outside of the normal Stealthwatch upgrade process, so you can update them more frequently. You do not have to update your Stealthwatch system in order to install these apps. You access installed apps from within the SMC Web App using the Dashboards menu. The apps you can view in the SMC Web App depends on your user permissions.

Refer to the following table to learn about the possible app statuses.

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 Flexera.

<table>
<thead>
<tr>
<th>Status</th>
<th>Definition</th>
<th>Action to Take</th>
</tr>
</thead>
<tbody>
<tr>
<td>UpToDate</td>
<td>Your installed app is the most current version.</td>
<td>No action is required.</td>
</tr>
<tr>
<td>UpdateAvailable</td>
<td>You have upgraded to a new version of Stealthwatch. Your existing app is</td>
<td>If you desire, go to Flexera to download and install the latest version (this will</td>
</tr>
<tr>
<td>Status</td>
<td>Definition</td>
<td>Action to Take</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>supported by this version of Stealthwatch, but a new version of this app is available.</td>
<td>replace your existing version).</td>
<td></td>
</tr>
<tr>
<td>UpgradeRequired</td>
<td>You have upgraded to a new version of Stealthwatch, and your existing app is not supported by the Stealthwatch version you are now using.</td>
<td>To continue using this app, go to Flexera to download and install the latest version (this will replace your existing version).</td>
</tr>
<tr>
<td>AppNotSupported</td>
<td>You have upgraded to a new version of Stealthwatch. This app may no longer be supported by the version 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.</td>
<td>Go to Flexera to see if a new version has been released.</td>
</tr>
<tr>
<td>Error</td>
<td>The installation, upgrade, or removal process for the associated app has not successfully completed.</td>
<td>Contact Cisco Stealthwatch Support (see the last section in this document for support contact information). A partial installation, upgrade, or removal of this app may have occurred. If so, this must be corrected.</td>
</tr>
</tbody>
</table>

**ISE Integration Enhancements**

**Changed the process to get pxGrid client certificates**

Starting with v7.0, Stealthwatch only imports client certificates created with a Certificate Signing Request (CSR) generated from Stealthwatch Central Management. See the Configuring Cisco ISE or ISE-PIC guide for details.
If you are upgrading from Stealthwatch v6.10.x, your pxGrid client certificates will remain and can be used to establish the connection with ISE. However, it's recommended to recreate your pxGrid client certificates with a CSR for security purposes.

Integration Options

Stealthwatch extends the integration with pxGrid and adds more capabilities and topics of information that can be used to obtain data and interact with ISE. These integration options are now configurable and can be turned on or off to better fit your system's needs.

The ISE configuration page includes the following integration options:

- Adaptive Network Control (ANC)
- Static TrustSec Classifications
- User Sessions

ISE connection status now shows you the status of connection to pxGrid and the status of the subscription to enabled topics of information.

TrustSec Security Group Tags

Stealthwatch v7.0 allows you to obtain TrustSec static endpoint classifications (IP-to-SGT bindings) from ISE in addition to previously available dynamic TrustSec classifications from user sessions. This allows augmentation of flows with a Security Group Tag (TrustSec ID) and a Security Group Name (TrustSec Name) in environments where TrustSec context is not available from the authentication process (statically classified endpoints like data center servers, topology based classifications, context learned by ISE from external systems via SXP process, etc). See the Overview of TrustSec documentation for more information about SGTs.

Changed Mitigation Actions

ANC policies have replaced the previous quarantine and unquarantine feature. You can now apply ANC policies to the endpoint and change the endpoint authorization status on the network according to the rules and policies configured on ISE. You manage Mitigation Actions using the ANC policies option on the Host Summary component of the Investigation a Host page. See the Setup ANC documentation for more information about setting up ANC policies in ISE.

To apply an ANC policy to a host, click Edit next to ISE ANC policies on Host Summary component. The ANC policies panel will open, which shows all ISE clusters configured in the host domain, along with information about available ANC policies. The ANC
policies drop-down will be available for ISE clusters where applying an ANC policy is possible.

EAP Chaining Sessions Support

Stealthwatch now supports the tracking of ISE sessions derived from EAP Chaining authentications. A prerequisite for successful detection of EAP Chaining session is successful user authentication in the EAP chaining process. Sessions with failed user authentications will not be by tracked by Stealthwatch.

Performance and Scalability

Stealthwatch v7.0 includes significant improvements related to ISE sessions processing. This allows support for up to 2,000,000 active sessions for high-end FC/SMC appliances platforms. See the ISE Integration Scalability Support document for more details.

UCS Hardware

Stealthwatch is available on the latest generation of UCS hardware (M5). For compatible model numbers and specifications, please refer to Cisco.com or contact your local Cisco Partner.

Update your firmware using Stealthwatch firmware and the Stealthwatch Update Guide. Do not use the standard UCS firmware update information posted on Cisco.com.

UDP Director

The M5 UDP Director includes a dual rate 1 or 10G copper management/ingress/egress port. Utilizing the 10G rate, the appliance may achieve up to 50% performance increase.
over the 1G rate.

- Given the port is copper, additional compatible network hardware is required for 10G rates over copper. Refer to the specification sheet for details.
- Your results may vary. The performance rate is impacted by packet size and number of forwarding rules.

Stealthwatch IDentity Appliance

If you have a Stealthwatch IDentity Appliance (ID-1000, ID-1100), replace the Lancope web certificate before you update the software to 7.0. Please refer to the Stealthwatch Update Guide for instructions.

New software update process

We have a new process for updating your Stealthwatch cluster from version 6.10.x to 7.0.0. The update includes the following:

- **Instructions:** Use the Stealthwatch Update Guide for complete instructions. It is important to follow the appliance update order and install the latest rollup patch file.
- **Appliance Admin interface:** You will install a patch (pre-SWU) file on your primary SMC.
- **Web interface:** You will install the patch (pre-SWU) and 7.0.0 SWU (software update file) on each appliance in the cluster.
- **New Appliance Update Order:** Make sure you update the appliances using the new order.
- **Certificates:** After you update the appliance software to 7.x, the default appliance identity certificate (previously Lancope) is replaced with a unique, self-signed appliance identity certificate. The appliance trust stores are updated automatically as part of this process. If the appliance uses a custom certificate, it will not be replaced.
- **Central Management:** After you update the appliance software to 7.x, you can manage your appliances from the primary SMC/Central Manager. See the Central Management section for details.
## Installation and Configuration

### Data Storage

The minimum data storage specifications have changed on new Virtual Edition (VE) appliance installations. The appliance data storage expands automatically when the appliance reboots. Refer to the [Stealthwatch Installation and Configuration Guide](#) for details and all resource requirements.

If you are upgrading your appliances to 7.0, review **Possible insufficient root partition space**

<table>
<thead>
<tr>
<th>Stealthwatch VE Model</th>
<th>Minimum Data Storage</th>
<th>Maximum Addressable Storage/ Hardware Equivalent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stealthwatch Management Console VE</td>
<td>125 GB</td>
<td>5.6 TB</td>
</tr>
<tr>
<td>Stealthwatch Management Console VE 2000</td>
<td>200 GB</td>
<td>7.2 TB</td>
</tr>
<tr>
<td>Flow Collector NetFlow VE</td>
<td>200 GB</td>
<td>1 TB</td>
</tr>
<tr>
<td>Flow Collector NetFlow VE 2000</td>
<td>600 GB</td>
<td>2 TB</td>
</tr>
<tr>
<td>Flow Collector NetFlow VE 4000</td>
<td>1.5 TB</td>
<td>7.2 TB</td>
</tr>
<tr>
<td>Flow Collector sFlow VE</td>
<td>100 GB</td>
<td>1 TB</td>
</tr>
<tr>
<td>Flow Collector sFlow VE 2000</td>
<td>600 GB</td>
<td>2 TB</td>
</tr>
<tr>
<td>Flow Collector sFlow VE 4000</td>
<td>1.5 TB</td>
<td>7.2 TB</td>
</tr>
<tr>
<td>Flow Sensor</td>
<td>60 GB</td>
<td></td>
</tr>
<tr>
<td>UDP Director</td>
<td>60 GB</td>
<td></td>
</tr>
</tbody>
</table>
Appliance Setup Tool

The Appliance Setup Tool has been updated so that new appliances can be configured with the following:

- **Passwords:** You will be prompted to change the default passwords for admin, root, sysadmin as part of the Appliance Setup Tool for new appliances.

  !important If any existing appliances are using default passwords, we strongly recommend that you change those passwords immediately.

- **Central Management:** You will be prompted to assign your appliance to a Central Manager, which is your Stealthwatch Management Console. See the Central Management section for details.

Time Zone UTC

All Stealthwatch appliances use Coordinated Universal Time (UTC) in 7.0.0.

- UTC will be used for displaying time and reporting events.
- The time zone cannot be changed.
- At least 1 NTP server is now required for each appliance.

USGv6 Certification

Stealthwatch is certified with USGv6 certification with basic IPv6 management port addressability. If you enable basic IPv6 addressing, you will still be required to provide an IPv4 address for your appliances until further components are implemented for IPv6.

Central Management

When your appliances are managed by Central Management, you can review their status and manage the following from one dashboard:

- edit appliance configuration
- update software
- create backup configuration files
- view audit logs
- reboot
- shut down
- review license status
Update Manager

The Update Manager replaces the System Management page used in v6.10.x

The Update Manager and software update process are available after you update all appliances to software v7.0.x. This new function cannot be used to upgrade an appliance from v6.10.x.

- **Patches**: Upload individual rollup patches or common patches for your appliances. See the Patch Readme file for details.
- **Software Update Files**: Upload individual SWU files for each appliance type.
- **Instructions**: Use the *Stealthwatch Software Update Guide* for complete instructions. It is important to follow the appliance update order and install the latest rollup patch file.

Certificates and Trust Store

Use Central Management to view and update your certificates for each appliance. Use Stealthwatch Online Help for instructions.

- **Certificate Signing Request (CSR)**: Use Central Management to generate the certificate signing request if you’re replacing the appliance identity or adding a client identity. You no longer need to generate a private key. The private key is generated as part of the CSR process.
- **Appliance Identity**: The appliance identity certificate is used for communication between Stealthwatch appliances. You can view the current appliance identity certificate or update the appliance identity certificate using SSL/TLS Appliance Identity.
• **Client Identity:** The client identity certificates are used for communication between external services such as Cisco Identity services (ISE). You can view the SMC client identity certificates or add client identity certificates using Additional SSL/TLS Client Identities.

• **Trust Store:** When you add a certificate to an appliance trust store, you are allowing communication with that identity, whether it is another Stealthwatch appliance or an external service.

**Stealthwatch Cloud: Early Access**

Stealthwatch Cloud: Early Access (SWC: Early Access) is time-limited functionality that expires after October 31, 2018 (the end date). SWC: Early Access allows you to send network telemetry data to the Stealthwatch cloud-based infrastructure, and receive host classification suggestions on the SMC. You enable this feature by selecting **Enable SWC Early Access** in the Central Manager. You review the host classification suggestions by clicking **Review Suggested Classification (BETA)** from the Host Group Management page.

After the end date, the feature is disabled for all users. Based on your Stealthwatch version, the following happen:

• In version 7.0.0, if you select **Enable SWC Early Access**, network telemetry is sent to the Stealthwatch cloud-based infrastructure, but not analyzed. The cloud-based infrastructure automatically deletes this network telemetry after 5 days. Enabling or disabling SWC: Early Access has **no negative effect** on your system. If you click **Review Suggested Classification (BETA)**, the system redirects you to a page with a 404 error, stating that the page could not be found.

• In versions greater than 7.0.0, the **Enable SWC Early Access** checkbox and **Review Suggested Classification (BETA)** button no longer appear.

The Stealthwatch Host Classifier app, available in the future, replicates the host classification suggestion functionality provided by SWC: Early Access. Contact your sales associate for more information.

**Installing the Stealthwatch Desktop Client**

As of Stealthwatch v7.0, Oracle Java will no longer be used to install and open Stealthwatch Desktop Client.

Use the following instructions to install the Stealthwatch Desktop Client using Windows or macOS. Note the following:
- You can locally install different versions of Stealthwatch Desktop Client.
- If you want to access multiple versions of Stealthwatch Desktop Client, you will need a different executable file for each SMC.
- If you are using both a primary and a secondary SMC, you will need to log off one SMC before you can log in to the other SMC.
- You can have different versions of Stealthwatch Desktop Client open simultaneously.
- When you update to a later version of Stealthwatch, you will need to install the new version of Stealthwatch Desktop Client.
- If you have Stealthwatch Desktop Client and update to 7.0.x or later, you can no longer use Oracle Java with Stealthwatch Desktop Client.

Install the Desktop Client Using Windows

- You must have sufficient rights to install Stealthwatch Desktop Client.
- Stealthwatch Desktop Client requires a 64-bit operating system. It cannot run on a 32-bit operating system or Linux.

1. Click Desktop Client in the upper right corner of any page in the Stealthwatch Web App.
2. Click the .exe file to begin the installation process.
3. Follow the steps in the wizard to install the Stealthwatch Desktop Client.
4. On your desktop, click the Stealthwatch Desktop Client icon.
5. Enter the SMC user name and password.
6. Enter the SMC server name or IP address (IPv4 or IPv6).
7. Follow the on-screen prompts to open the Desktop Client and trust the appliance identity certificate.

Change the memory size

You can change how much Random Access Memory (RAM) to allocate on your client computer to run the Stealthwatch Desktop Client interface. Consider a larger memory allocation if you work with many open documents or large data sets (such as flow queries with over 100k records).

1. In Windows Explorer, go to your home directory.
2. Open these folders: AppData > Roaming > Stealthwatch.
You may need to search "Stealthwatch" if the folder is hidden.

3. In the Stealthwatch directory, open the folder that contains the desired Stealthwatch version.

4. Open the `application.vmoptions` file using an appropriate editing application to begin editing. (This file is created after you open the Stealthwatch Desktop Client for the first time.)

**Minimum Memory Size (Xms):** We recommend that you allocate no less than 512 MB. This number is listed in the third line of the file.

For editors that display the content in one continuous line, refer to the number highlighted in the image below to see which number represents the minimum memory size.

```
# Enter one VM parameter per line# Use -Xms to specify the initial Java heap size and Use -Xmx to specify the maximum heap size.
Xms512m
```

**Maximum Memory (Xmx):** You can allocate up to half the size of your computer's RAM for the maximum memory size. This number is listed in the fourth line of the file.

For editors that display the content in one continuous line, refer to the number highlighted in the image below to see which number represents the maximum memory size.

```
# Enter one VM parameter per line# Use -Xms to specify the initial Java heap size and Use -Xmx to specify the maximum heap size.
Xmx2048m
```

**Use whole numbers.** For example, enter Xmx512m, not Xmx0.5m.

- If you notice that the Stealthwatch Desktop Client appears to "hang" frequently, try increasing the memory size.
- If you receive an error message involving Java, try selecting a lower memory allocation.

**Install the Desktop Client Using macOS**

- You must have sufficient rights to install Stealthwatch Desktop Client.
- Stealthwatch Desktop Client requires a 64-bit operating system. It cannot run on a 32-bit operating system or Linux.
1. Click **Desktop Client** in the upper right corner of any page in the Stealthwatch Web App.

2. Click the .dmg file to begin the installation process.

   An icon and folder are displayed on your monitor, as shown below.

   ![Desktop Client icon and folder](image)

3. Drag the Stealthwatch Desktop Client icon into the Application folder.

   The icon is added to the Launchpad.

4. On your desktop, click the Stealthwatch Desktop Client icon.

5. Enter the SMC user name and password.

6. Enter the SMC server name or IP address (IPv4 or IPv6).

7. Follow the on-screen prompts to open the Desktop Client and trust the appliance identity certificate.

**Change the memory size**

You can change how much Random Access Memory (RAM) to allocate on your client computer to run the Stealthwatch Desktop Client interface. Consider a larger memory allocation if you work with many open documents or large data sets (such as flow queries with over 100k records).

1. In Finder, go to your home directory.

2. Open the Stealthwatch folder.

3. In the Stealthwatch directory, open the folder that contains the desired Stealthwatch version.

4. Open the application.vmoptions file using an appropriate editing application to begin editing. (This file is created after you open the Stealthwatch Desktop Client for the first time.)

   **Minimum Memory Size (Xms):** We recommend that you allocate no less than
512 MB. This number is listed in the third line of the file.
For editors that display the content in one continuous line, refer to the number highlighted in the image below to see which number represents the minimum memory size.

Maximum Memory Size (Xmx): You can allocate up to half the size of your computer’s RAM for the maximum memory size. This number is listed in the fourth line of the file.
For editors that display the content in one continuous line, refer to the number highlighted in the image below to see which number represents the maximum memory size.

Use whole numbers. For example, enter Xmx512m, not Xmx0.5m.

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 email: tac@cisco.com
  - For phone support: 1-800-553-2447 (U.S.)
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 7.0.0

<table>
<thead>
<tr>
<th>Defect</th>
<th>Description</th>
<th>LSQ</th>
</tr>
</thead>
<tbody>
<tr>
<td>SWD-7700</td>
<td>The Flow Collection Trend chart had gaps due to TextCopyHandler failing to read files at /lancope/var/smc/tmp folder. Resolved an issue where scheduled reports would terminate existing SMC data loading processes under certain conditions.</td>
<td>LSQ-2727</td>
</tr>
<tr>
<td>SWD-8115</td>
<td>Multiple instances of the process &quot;acpi_pad&quot; was causing the system to become non-responsive. We blacklisted the &quot;acpi_pad&quot; process to fix this issue.</td>
<td>LSQ-2836</td>
</tr>
<tr>
<td>SWD-8142</td>
<td>The Database backup is generating errors at the final stage of the process. Improvements have been added to repeat the Vertica backup process in case of resync errors.</td>
<td>LSQ-2838</td>
</tr>
<tr>
<td>SWD-8773</td>
<td>Upgraded mongodb from v2.6.8 to v3.10.15 to take advantage of performance improvements.</td>
<td>LSQ-3012</td>
</tr>
<tr>
<td>SWD-9128</td>
<td>Temporary files for flow stats were deleted when disk space was less than 75%. This code was removed in order to let the code that checks disk usage handle any necessary file removals.</td>
<td>LSQ-3123</td>
</tr>
<tr>
<td>SWD-9138</td>
<td>&quot;String index out of range&quot; error in Offline Activation dialog. Improved exception handling to address the error and</td>
<td>LSQ-3124</td>
</tr>
<tr>
<td>Defect</td>
<td>Description</td>
<td>LSQ</td>
</tr>
<tr>
<td>----------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>SWD-9258</td>
<td>added an additional condition to verify the presence of a dash symbol.</td>
<td>LSQ-3141</td>
</tr>
<tr>
<td>SWD-9444</td>
<td>The Flow Collector Engine failed to connect a router mitigation device when using SSH. Updated the engine code responsible for building and maintaining SSH mitigation sessions.</td>
<td>LSQ-3196</td>
</tr>
<tr>
<td>SWD-9445</td>
<td>The Flow Collector engine had a SIGSEGV error at pool_exit in process_message. A memory leak was found and fixed related to the deletion of exporters, and extra protection was put into place in the handling of the Service Bandwidth data structures.</td>
<td>LSQ-3176</td>
</tr>
<tr>
<td>SWD-9446</td>
<td>A quotation mark in the application detail column caused an error when exporting a flow table to a CSV file. The application detail fields were updated to handle quotation marks.</td>
<td>LSQ-3086</td>
</tr>
<tr>
<td>SWD-9490</td>
<td>The export button was cut off on the Flow Search page. Updated the UI to handle resizing the browser window.</td>
<td>LSQ-3223</td>
</tr>
<tr>
<td>SWD-9502</td>
<td>The &quot;more details&quot; link on the UDP Director admin page disappeared once the page loaded. Fixed the hyperlink to be consistent during and after page load.</td>
<td>LSQ-3224</td>
</tr>
<tr>
<td>SWD-9503</td>
<td>The SMC 1000 was running out of memory which caused Vertica to crash. Fixed the memory leak.</td>
<td>LSQ-3228</td>
</tr>
<tr>
<td>SWD-9515</td>
<td>The Flow Collector 5020 failed to load the 10G driver. Modified the grub configuration files to allow the Intel</td>
<td>LSQ-3235</td>
</tr>
<tr>
<td>Defect</td>
<td>Description</td>
<td>LSQ</td>
</tr>
<tr>
<td>---------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>SWD-9520</td>
<td>10G network card to work with the Jessie kernel.</td>
<td>LSQ-3346</td>
</tr>
</tbody>
</table>
| SWD-9524 | Log rotation for vertica.log was not working.  
Added a daily cron job to cleanup any backup vertica logs in the target directory that haven’t changed in 30 days. | LSQ-3207|
| SWD-9559 | The UDP Director device information column was not populating when the Management Channel Down alarm triggered.  
Added the device type to the system_alarm table. | LSQ-3208|
| SWD-9564 | The Flow Collector engine had a SIGSEGV error at search_threat_host.  
Reworked threat feed code to minimize the locking time of the processing threads.                                                                 | LSQ-3237|
| SWD-9568 | Vertica hung at "SafetyShutdown".  
Added code to monitor vertica and restart it if the process is up but the DB is not responsive.                                                                                                       | LSQ-3228|
| SWD-9577 | The hostname field was missing from the HostAlarm structure in the MIB.  
Added the missing field.                                                                                                                      | LSQ-3209|
<p>| SWD-9607 | Added the &quot;Peer Host Groups&quot; option to the Manage Columns menu for the Top Conversations table.                                                                                                            | LSQ-3266|
| SWD-9692 | Fixed the Traffic by Peer Host Group display that was using the wrong timestamp for some archive hour settings.                                                                                             | LSQ-3277|</p>
<table>
<thead>
<tr>
<th>Defect</th>
<th>Description</th>
<th>LSQ</th>
</tr>
</thead>
<tbody>
<tr>
<td>SWD-9702</td>
<td>Modified the Flow Collector engine to handle ICMP type and code sent in the NetFlow source port field instead of destination port.</td>
<td>LSQ-3175</td>
</tr>
<tr>
<td>SWD-9732</td>
<td>No indication when the SMC server failed to load because of an invalid smc_failover.xml file. Added the appropriate log to the SMC log file.</td>
<td>LSQ-3228</td>
</tr>
<tr>
<td>SWD-9873</td>
<td>The alarm count was mismatched from the Alarming Hosts component on the Security Insight Dashboard and the alarms on the host list view. Updated the help text pop-up to explain that the number in the Alarming Host component displays the number of hosts receiving alarms since the last reset hour. Clicking on the alarm number will navigate to a host list view with an alarm category filter applied. These two numbers can be different.</td>
<td>LSQ-3330</td>
</tr>
<tr>
<td>SWD-9913</td>
<td>Updated the Cognitive Analytics integration to work with trial licenses.</td>
<td>LSQ-3675</td>
</tr>
<tr>
<td>SWD-9934</td>
<td>Queries for security events failed with a Vertica error. Updated the code to finish installing Vertica default packages.</td>
<td>LSQ-3578</td>
</tr>
<tr>
<td>SWD-9983</td>
<td>The database storage &quot;Worst Case&quot; value for &quot;capacity in days&quot; and &quot;remaining days&quot; was incorrect. Fixed the code so that the values are no longer negative.</td>
<td>LSQ-3367</td>
</tr>
<tr>
<td>SWD-9996</td>
<td>The “Not Matched” field in the output.log did not increment when the source/destination IP address mismatched the forwarding rules configuration on the UDP Director. A fix has been provided to increase the “Not Matched” count.</td>
<td>LSQ-3370</td>
</tr>
<tr>
<td>Defect</td>
<td>Description</td>
<td>LSQ</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>SWD-10008</td>
<td>The &quot;Interface Service Traffic&quot; graph was missing data. Adjusted the query for the graph to fix a Vertica database issue.</td>
<td>LSQ-3335</td>
</tr>
<tr>
<td>SWD-10101</td>
<td>The SMC did not have enough memory allocated for Tomcat. Separated the JVM settings so that Tomcat memory allocation varies depending on the appliance.</td>
<td>LSQ-3305     LSQ-3453</td>
</tr>
<tr>
<td>SWD-10119</td>
<td>Host_group_application_traffic had an overflow for BPS values. Fixed the case where the SMC was inserting too many or too few primary data points, which caused the original consolidation value to record wrong values in Vertica.</td>
<td>LSQ-3397     LSQ-3433</td>
</tr>
<tr>
<td>SWD-10129</td>
<td>Associated flows information was incorrect. Updated SETI and the SMC Web App interface online help to have the correct associated flows information.</td>
<td>LSQ-3415</td>
</tr>
<tr>
<td>SWD-10147</td>
<td>Updated packet query logging.</td>
<td>LSQ-3418</td>
</tr>
<tr>
<td>SWD-10202</td>
<td>Flow information was not showing up when using a Cisco 3504 Wireless LAN Controller. Previously, the engine automatically assigned Interface #1 to flows missing Input and Output SNMP Interface IDs. Because of potential conflicts with an actual Interface #1, we decided to use INT_MAX for this assignment.</td>
<td>LSQ-3432</td>
</tr>
<tr>
<td>SWD-10239</td>
<td>DBNodeRetentionManager was not waiting long enough between partition drops which caused all partitions to be dropped. A back-off algorithm was implemented in the retention code to allow enough time for the disk space to be freed between partition drops.</td>
<td>LSQ-3444</td>
</tr>
<tr>
<td>Defect</td>
<td>Description</td>
<td>LSQ</td>
</tr>
<tr>
<td>---------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>SWD-10284</td>
<td>The Flow Collector 5000 engine had SIGSEGV error at various functions. Added more data input validation on Information Elements so the engine emits decode errors instead of crashing.</td>
<td>LSQ-3454</td>
</tr>
<tr>
<td>SWD-10329</td>
<td>Updated Security Group Tags (SGT) information in the SMC Web App interface online help.</td>
<td>LSQ-3461</td>
</tr>
<tr>
<td>SWD-10348</td>
<td>UDP Director failed to update ARP status for a host. Added a ping from the UDP Director to check disabled hosts in order to update the ARP status.</td>
<td>LSQ-3407</td>
</tr>
<tr>
<td>SWD-10387</td>
<td>Increased the default buffer length for the UDP Director to reduce &quot;Last Dropped&quot; counts.</td>
<td>LSQ-3463</td>
</tr>
<tr>
<td>SWD-10391</td>
<td>Added a script to set the ethX rx buffers to the maximum allowed value (typically 4096) on physical UDP Directors to improve performance.</td>
<td>LSQ-3463</td>
</tr>
<tr>
<td>SWD-10423</td>
<td>The Admin Interface UI hangs after clicking &quot;Test&quot; on the Remote File System page. Added better error handling for the Admin UI.</td>
<td>LSQ-3483</td>
</tr>
<tr>
<td>SWD-10436</td>
<td>The Flow Collector diagnostic pack stored too many log files. Updated the diagnostic pack to only contain the vertica.log.</td>
<td>NA</td>
</tr>
<tr>
<td>SWD-10444 SWD-10519</td>
<td>Updated the database queries to use AVG function to avoid the sum overflow problems.</td>
<td>LSQ-3487</td>
</tr>
<tr>
<td>SWD-10561</td>
<td>The engine had a SIGSEGV error in update_app_definitions. Ensured that all resource memory pool deletions are fol-</td>
<td>LSQ-3529</td>
</tr>
<tr>
<td>Defect</td>
<td>Description</td>
<td>LSQ</td>
</tr>
<tr>
<td>----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td></td>
<td>owed by setting the variable using the memory to NULL.</td>
<td></td>
</tr>
<tr>
<td>SWD-10570</td>
<td>The Flow Collector engine had an overflow when calculating BPS values. Bytes and packets value handling was modified to perform data validation and ensure the average packet size is 65535 bytes or less.</td>
<td>LSQ-3424</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LSQ-3433</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LSQ-3397</td>
</tr>
<tr>
<td>SWD-10593</td>
<td>The unlicensed feature message was being displayed for the Flow Sensor. Changed the default setting for the message to show the appropriate status.</td>
<td>LSQ-3486</td>
</tr>
<tr>
<td>SWD-10647</td>
<td>Top Peers flipping the client/server when selecting &quot;Flows&quot;. Modified the code to snow swap hosts when creating a flow filter from Top Peers.</td>
<td>LSQ-3554</td>
</tr>
<tr>
<td>SWD-10658</td>
<td>Removed &quot;Inbound&quot; from the legend for two charts on the Interface Traffic Dashboard.</td>
<td>LSQ-3335</td>
</tr>
<tr>
<td>SWD-10779</td>
<td>User authentication failed due to login file descriptors not being closed. Updated the code to close the file descriptors after a user logs out.</td>
<td>LSQ-3579</td>
</tr>
<tr>
<td>SWD-10893</td>
<td>The engined crashed with the error &quot;Thread interrupted&quot; while processing flows. Updated the engine to handle situations where the flow classification threads get backed up temporarily.</td>
<td>LSQ-3600</td>
</tr>
<tr>
<td>SWD-11065</td>
<td>Improvements were made in the calculations of data byte counts in the per-minute flow statistics.</td>
<td>LSQ-3582</td>
</tr>
<tr>
<td>Defect</td>
<td>Description</td>
<td>LSQ</td>
</tr>
<tr>
<td>----------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>SWD-11123</td>
<td>DBNodeRetentionManager was not dropping the large partitions causing new flow data to not be inserted. Modified retention code to drop any invalid partitions (those with dates before 1980) at each retention check. Any drops of these partitions will be logged with a warning &quot;Dropped invalid partition for &lt;table name&gt;&quot;. The code also drops up to 5 partitions each retention period when over the disk usage threshold. Disk space is checked after each drop and when usage drops back below threshold, no more partitions are dropped for that period.</td>
<td>LSQ-3623</td>
</tr>
<tr>
<td>SWD-11124</td>
<td>Vertica was inserting data when the database disk space was full, causing the system to crash. Modified the Flow Collector 5000 engine code to query Vertica for disk usage over the database channel. This allows the engine to stop database inserts when disk usage reaches the critical level on the database node even if the communication channel is down.</td>
<td>LSQ-3623</td>
</tr>
<tr>
<td>SWD-11197</td>
<td>The Flow Collector 5200 engine was running out of memory. The fix is to limit the number of processing threads based on the available memory. The calculated process_instance_count will be limited to 13 on a Flow Collector 5200 series appliance. This value can still be manually set in lc_thresholds.txt.</td>
<td>LSQ-3600</td>
</tr>
<tr>
<td>SWD-11198</td>
<td>Multiple errors causing the Flow Collector engine to crash. Fixed an out of bounds array reference that could corrupt memory and lead to a crash.</td>
<td>LSQ-3600</td>
</tr>
<tr>
<td>SWD-11243</td>
<td>Exporter flows could not be processed by the engine due to changes in the template.</td>
<td>LSQ-3647</td>
</tr>
<tr>
<td>Defect</td>
<td>Description</td>
<td>LSQ</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td></td>
<td>Removed support the old Flow Sensor Initiator field &quot;Information Element 68&quot;.</td>
<td></td>
</tr>
<tr>
<td>SWD-11480</td>
<td>Removed the code to swap Security Group Tag IDs when client and server were swapped in the engine (LSQ-3650).</td>
<td>LSQ-3650</td>
</tr>
<tr>
<td>SWD-11650</td>
<td>The Flow Sensor was missing flowsensor.xml after install.ian</td>
<td></td>
</tr>
<tr>
<td>SWD-11722</td>
<td>Updated the start_fs process so that it will write out a default flowsensor.xml when the service is started.</td>
<td>LSQ-3725  LSQ-3729</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Defect Number</th>
<th>Description</th>
<th>Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>SWD-7627</td>
<td>If you reboot your Flow Collector, it deletes all alarm history; however, if you replace your Flow Collector, the new Flow Collector retains the alarm history from the old Flow Collector instead of deleting it. Since the alarming host widgets (which display the number of hosts receiving alarms since the last reset hour for a specific category) on the Security Insight Dashboard and Host Group page then do not update until the next reset hour, you may see a discrepancy between these values and the alarm values in the Hosts table on the Host List View.</td>
<td>None currently available.</td>
</tr>
<tr>
<td>SWD-7655</td>
<td>The generation of a diagnostics pack may fail in large systems as a result of timing out.</td>
<td>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.</td>
</tr>
<tr>
<td>SWD-8197</td>
<td>The Flow Sensor was not detecting enough applications.</td>
<td>To provide more accurate application classification, we updated the third-party library for Application Iden-</td>
</tr>
<tr>
<td>Defect Number</td>
<td>Description</td>
<td>Workaround</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
<td>------------</td>
</tr>
<tr>
<td></td>
<td>tification. 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.</td>
<td></td>
</tr>
<tr>
<td>SWD-8673</td>
<td>SystemConfig special character fonts look bad when using the SecureCRT client in ANSI mode.</td>
<td>To overcome this, disable ANSI Color when connecting or use a different client to view the SystemConfig script.</td>
</tr>
<tr>
<td>SWD-9052</td>
<td>Offline license activation failing or &quot;Storage Binding Break&quot; error</td>
<td>This error may occur if you moved a virtual machine, uploaded a license more than once, or if the license is corrupted. Please contact Stealthwatch Customer Community for assistance.</td>
</tr>
</tbody>
</table>
| SWD-9563     | When you log in to the Stealthwatch Web App using Internet Explorer v11 and at any point you refresh the Home page, the Desktop Client drop-down arrow and the three navigation icons to the left of this list (top right corner of page) disappear. These three icons include the following:  
  - Search (magnifying glass icon)  
  - Help (person icon)  
  - Global Settings (geer icon)  
  Additionally, the fonts look different from | Close the browser and log in again. |
<table>
<thead>
<tr>
<th>Defect Number</th>
<th>Description</th>
<th>Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>SWD-11822</td>
<td>Stealthwatch has made a modification to interface API encoding that takes</td>
<td>In order for your integration with this API to function correctly, you must</td>
</tr>
<tr>
<td>(LVA-664)</td>
<td>effect beginning with v7.0. When configuring a query parameter for the related</td>
<td>do the following:</td>
</tr>
<tr>
<td></td>
<td>endpoints, you can no longer use un-escaped characters within the URI.</td>
<td>For all endpoints related to the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/tenants/{tenantId}/devices/{device_id}/exporters/{exporterIp}/interfaces/{interfaceId}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Filters such as start or end time need to be formatted as this:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>filter%5bstartTime%5d</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Not this:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>filter[startTime]</td>
</tr>
<tr>
<td>SWD-11885</td>
<td>The underscore character is not supported for the TrustSec Name field on the</td>
<td>To overcome this:</td>
</tr>
<tr>
<td></td>
<td>Flow Search and Custom Security Event pages.</td>
<td>• Do not use &quot;_&quot; in your TrustSec (Security Group) names.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Use the TrustSec ID instead of the TrustSec name when using the Flow Search</td>
</tr>
<tr>
<td></td>
<td></td>
<td>and to create the Custom Security Event.</td>
</tr>
<tr>
<td>Defect Number</td>
<td>Description</td>
<td>Workaround</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SWD-11929</td>
<td>The SMC desktop client does not launch over IPv6 on Mac.</td>
<td>None currently available.</td>
</tr>
<tr>
<td>SWD-12028</td>
<td>The SMC fails to apply ANC Policies with dash, &quot;-&quot;, characters in the name.</td>
<td>To overcome this, do not use &quot;-&quot; in your ANC Policy names.</td>
</tr>
<tr>
<td>SWD-12051</td>
<td>The API documentation link is incorrect in the SMC Web App interface online help.</td>
<td>Go <a href="#">here</a> to access API documentation.</td>
</tr>
<tr>
<td>SWD-12141</td>
<td>When installing the pre-SWU patch using the SMC System Management page, the Update Status may continue to show &quot;Waiting to install.&quot;</td>
<td>The message might not clear, but it does not block the update. Check the log to confirm the pre-SWU patch was installed successfully. Make sure you follow the Finalize procedure in the <a href="#">Stealthwatch Update Guide</a>.</td>
</tr>
</tbody>
</table>
| 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 |
<table>
<thead>
<tr>
<th>Defect Number</th>
<th>Description</th>
<th>Workaround</th>
</tr>
</thead>
</table>
| SWD-13181     | The Flow Collector database and engine private network IP addresses cannot be changed. Changing these IP addresses will break communications. | • Make sure the Appliance Status is shown as Up.  
• Check the other appliance trust stores 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.  
|               | The Flow Collector database and engine use private network IP addresses to communicate. The private network IP addresses are as follows:  
Engine: 169.254.42.100  
Database: 169.254.42.101  
If you've changed these IP addresses, change them back to the defaults or contact [Cisco Stealthwatch Support](#) before you start the update. |
<table>
<thead>
<tr>
<th>Defect Number</th>
<th>Description</th>
<th>Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHOPIN-25123</td>
<td>On a pair of dual SMCs, the secondary SMC will not connect to Cognitive Analytics after configuration. This does not interfere with the Flow Collector receiving data and the primary SMC connects to Cognitive and displays the widgets properly.</td>
<td>If the primary SMC fails, the secondary SMC will connect to Cognitive Analytics and display the widgets. When the original primary SMC comes up, both SMCs will successfully connect to Cognitive. To connect the secondary SMC to Cognitive, you will need to swap the secondary and primary SMC, then register to Cognitive. You can swap the SMCs back to the original configuration after confirming registration.</td>
</tr>
<tr>
<td>NA</td>
<td>On the Flow Sensor VE, “Export Application Identification” is off by default.</td>
<td>To enable application identification, this advanced setting will need to be manually selected.</td>
</tr>
<tr>
<td>NA</td>
<td>Due to changes in the cipher suite properties from TLS v1.2 to TLS v1.3, the Key Exchange and Authentication Algorithm properties will display as N/A in the Flow Search.</td>
<td>Full audit capabilities for TLS v1.3 will be added in a future release.</td>
</tr>
<tr>
<td>NA</td>
<td>If a Stealthwatch user has their privileges lifted or demoted (ex. Read Only to Read/Write or vice versa), it will take up to 30 minutes to propagate the change to the Cognitive Analytics system.</td>
<td>None currently available.</td>
</tr>
<tr>
<td>NA</td>
<td>If a user logs in to multiple Stealthwatch</td>
<td>To overcome this:</td>
</tr>
<tr>
<td>Defect Number</td>
<td>Description</td>
<td>Workaround</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
<td>------------</td>
</tr>
</tbody>
</table>
|               | systems, they can't log in to the second system within Cognitive Analytics. | • Wait 30 minutes for the first login to expire  
• Log out of Cognitive Analytics on the first system |
Reported 6.10.X > 7.0 Upgrade Issues

The following items are issues that have been reported in the field and are currently being investigated by the Stealthwatch team.

<table>
<thead>
<tr>
<th>Defect/LSQ</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SWD-13025/LSQ-4083</td>
<td>Customer is upgrading from 6.10.2 with latest patches applied. Has primary and secondary SMC and other devices. Applied update patches in the correct order, but all devices are appearing in the Disconnect From Cluster column during finalization.</td>
</tr>
<tr>
<td>LSQ-4159 LSQ-4170</td>
<td>Customer experiences &quot;Expired cert in chain&quot; and &quot;server.crt has certs in incorrect format&quot;.</td>
</tr>
<tr>
<td>LSQ-4098 LSQ-4178 LSQ-4108</td>
<td>Customer experienced an issue, but the underlying cause was missed due to multiple failed attempts to upgrade.</td>
</tr>
<tr>
<td>SWD-13048/LSQ-4088</td>
<td>Unable to reproduce an issue with a successful update where the SMC did not show up in the finalize column.</td>
</tr>
<tr>
<td>SWD-12896/LSQ-4088</td>
<td>Unable to reproduce an issue where after &quot;successfully&quot; completing 7.0.0 Upgrade on two FCNFVEs, WebUI never responds.</td>
</tr>
<tr>
<td>SWD-12881 /LSQ-4177 LSQ-4130</td>
<td>After upgrade, the upgrade log history is lost. This is now a known issue, and pre-update backups must be made before upgrading. See the update note above.</td>
</tr>
<tr>
<td>SWD-13097/LSQ-4224</td>
<td>Customer upgraded the FCDB and the FC engines from 6.9.5 to 6.10.4. After upgrade both FCs are giving license errors: &quot;Missing license feature&quot; and are dropping all the flows.</td>
</tr>
</tbody>
</table>
Release Support Information

Official General Availability (GA) date for Release 7.0 is Jan. 30th, 2019.

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

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)