Cisco Stealthwatch

Update Guide 7.0.3
# Table of Contents

**Introduction** .................................................................................................................. 6
  - Overview ......................................................................................................................... 6
  - Audience ......................................................................................................................... 6
  - Terminology .................................................................................................................... 6
  - New Update Process ....................................................................................................... 7

**Before You Begin** .......................................................................................................... 8
  - Possible Insufficient Root Partition Space ................................................................. 8
  - Software Version ........................................................................................................... 8
  - Java ................................................................................................................................. 9
  - TLS .................................................................................................................................. 9
  - Default Credentials ....................................................................................................... 9
  - Port 5672 ....................................................................................................................... 10
  - Third Party Applications ................................................................................................ 10
  - Browsers ....................................................................................................................... 10
  - Hardware ....................................................................................................................... 10
  - Flow Sensor 4000 ......................................................................................................... 10
  - SMC ................................................................................................................................. 10
  - UDP Director .................................................................................................................. 11
  - Licensing ....................................................................................................................... 11
  - ISE or ISE-PIC ............................................................................................................... 11
  - Host Name ..................................................................................................................... 11
  - Domain Name ............................................................................................................... 11
  - NTP Server .................................................................................................................... 12
  - Time Zone ..................................................................................................................... 12
  - Custom Certificates ....................................................................................................... 12
  - Trust Store ..................................................................................................................... 13
  - Backing Up Your Appliances ....................................................................................... 13
### Backing up the Flow Collector Database

13

### Best Time to Update

14

1. **Software Update Files**

14

2. **All Appliances**

14

3. **SMCs and Flow Collectors**

14

4. **Communications**

14

### After the Update

16

1. **Upgrade Issue**

16

2. **Patch Installation**

16

### Alternative Access

17

1. **Hardware**

17

2. **Virtual Machines**

17

3. **Additional Option**

17

### Stealthwatch IDentity Appliances (A10)

19

1. **1. Update the Software**

19

2. **2. Review the Current Certificate**

19

3. **3. Create a New Certificate**

20

4. **4. Confirm the New Certificate**

20

5. **5. Enable the Certificate**

22

6. **6. Verify and Export**

22

7. **7. Install the New Certificate on your SMC**

23

### Update Overview

25

1. **New Process**

25

2. **Update Process Overview**

25

### 1. Review Your Cluster

26

1. **Best Practices**

26

2. **1. Review Your Managed Appliances**

27

3. **Add Appliances to Your Stealthwatch Cluster**

28

4. **Remove Appliances from Your Stealthwatch Cluster**

28

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Check Flow Sensor Settings</td>
<td>29</td>
</tr>
<tr>
<td>2. Confirm the Installed Software Version</td>
<td>31</td>
</tr>
<tr>
<td>3. Download the Patches and Update Files</td>
<td>33</td>
</tr>
<tr>
<td>Pre-SWU (Patch) Files</td>
<td>34</td>
</tr>
<tr>
<td>SWU Files</td>
<td>34</td>
</tr>
<tr>
<td>4. Back Up the Appliance Configuration</td>
<td>36</td>
</tr>
<tr>
<td>5. Create a Diagnostics Pack</td>
<td>37</td>
</tr>
<tr>
<td>6. Back Up the Flow Collector and SMC Databases</td>
<td>38</td>
</tr>
<tr>
<td>1. Disable SNMP Polling for an SMC</td>
<td>38</td>
</tr>
<tr>
<td>2. Trim the Flow Collector Database</td>
<td>39</td>
</tr>
<tr>
<td>1. Review your Database Storage Statistics</td>
<td>39</td>
</tr>
<tr>
<td>2. Trim the Interface Details</td>
<td>40</td>
</tr>
<tr>
<td>3. Trim Flow Details and CI Event Data</td>
<td>41</td>
</tr>
<tr>
<td>3. Back Up the Databases</td>
<td>41</td>
</tr>
<tr>
<td>4. Delete the Flow Collector Snapshots</td>
<td>44</td>
</tr>
<tr>
<td>5. Re-enable SNMP Polling in the SMC</td>
<td>44</td>
</tr>
<tr>
<td>7. Check the Available Disk Space</td>
<td>45</td>
</tr>
<tr>
<td>8. Install the Pre-SWU Patch on SMCs</td>
<td>46</td>
</tr>
<tr>
<td>9. Install the Pre-SWU Patch on Managed Appliances</td>
<td>48</td>
</tr>
<tr>
<td>10. Finalize the Pre-SWU Installation</td>
<td>50</td>
</tr>
<tr>
<td>11. Install the 7.0 Software Update</td>
<td>56</td>
</tr>
<tr>
<td>Use the New Update Order</td>
<td>56</td>
</tr>
<tr>
<td>Best Practices</td>
<td>58</td>
</tr>
<tr>
<td>Install the v7.0.3 Update on Managed Appliances</td>
<td>58</td>
</tr>
<tr>
<td>12. Log in to Central Management</td>
<td>61</td>
</tr>
<tr>
<td>13. Install v7.0.3 Patches</td>
<td>63</td>
</tr>
<tr>
<td>14. Log in to the SMC Desktop Client</td>
<td>64</td>
</tr>
<tr>
<td>Trust the Certificate in the SMC Desktop Client</td>
<td>64</td>
</tr>
<tr>
<td>Verify SMC Failover Roles</td>
<td>64</td>
</tr>
</tbody>
</table>
15. Update Stand-Alone or Disconnected Appliances ........................................ 67
   1. Check the Software Version ................................................................. 67
   2. Prepare the Appliance ........................................................................... 68
   3. Install the Pre-SWU ............................................................................. 68
   4. Install the v7.0.x SWU ........................................................................ 70
   5. Add the Appliance to Central Management ......................................... 71
      Best Practices ...................................................................................... 72
      Managed and Stand-Alone Requirements in Central Management ....... 73
      Add the Appliance to Central Management ......................................... 74

Contacting Support .................................................................................. 75
Introduction

Overview

Use this guide to update the following Stealthwatch appliances from v6.10.x to v7.0.3 (or a later version of 7.0.x):

- UDP Director (also known as FlowReplicator)
- Endpoint Concentrator
- Stealthwatch Flow Collector
- Stealthwatch Flow Sensor
- Stealthwatch Management Console (SMC)

For details on v7.0.3, refer to the Release Notes.

Audience

The intended audience for this guide includes network administrators and other personnel who are responsible for updating Stealthwatch products.

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."
New Update Process

We have a new process for updating your Stealthwatch appliances from version 6.10.x to v7.0.3 (or a later version of 7.0.x). The update includes the following:

- **Appliance Administration Interface**: installing a patch (pre-SWU) file on your primary SMC.
- **Web App Interface**: installing the patch (pre-SWU) and v7.0.x SWU (software update file) on each appliance in the cluster.
- **New Appliance Update Order**: After you install the pre-SWU, make sure you install the v7.0.x SWU following the instructions in this guide and using the new order.
- **Certificates**: After you update the appliance software to v7.0.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 all Stealthwatch appliances to v7.0.x, you can manage your appliances from the primary SMC/Central Manager.

For details on v7.0.3, refer to the [Release Notes](#).
Before You Begin

Before you begin the update process, review this guide to understand the process, as well as the preparation, time, and resources you'll need to plan for the update.

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 v7.0.3 (or a later version of 7.0.x), 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.

- If you are attempting to run a patch, you might need to uninstall one or more apps to free up space.

- **After the Update:** This guide provides instructions for checking the root partition after you update your appliances. Refer to the Log in to Central Management section or Update Stand-Alone or Disconnected Appliances for details.

Software Version

To update the appliance software to version v7.0.x, the appliance must have 6.10.2, 6.10.3, or a later version of 6.10.x installed. The instructions in this guide will show you how to check the software version on each appliance. It is also important to note the following:

- **Patches:** For each software version, make sure you install the latest patches on your appliances before you upgrade. For details, log in to the Stealthwatch 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 v6.10.4 (or the latest version of 6.10.x). Each update guide is available on the Customer Community or on Cisco.com.
• **Same Version:** Make sure all appliances are using the same software version. For example, if your SMC has v6.10.3 installed, the other appliances in your cluster need to have v6.10.3 installed.

• **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.

### 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.

### TLS

Stealthwatch requires TLS v1.1 or later.

### Default Credentials

**Port 5672** is used for RabbitMQ during the pre-SWU installation. We are using a temporary authentication file with default credentials, as follows:

- **User Name:** upgrade
- **Password:** @ist+ipsdishzsfadetidyprizecrag007hm

The temporary authentication file allows us to rebuild the trust stores during the update. Once the update is completed, the credentials are replaced.

For a brief amount of time between the pre-SWU installation and the v7.0.x update, the risk of exposure may increase. If your security restrictions do not permit default credentials, please contact [Cisco Stealthwatch Support](#) to set up custom credentials.
Port 5672

The Flow Collector, Flow Sensor, and UDP Director need to have open communication to the SMC on **port 5672**. The communication is encrypted, and TCP access is required. Refer to [Default Credentials](#) for related information.

If you encounter port errors during the update, make sure port 5672 is open, or contact your system administrator.

Third Party Applications

Stealthwatch does not support installing third party applications on appliances.

Browsers

- **Compatible Browsers**: Stealthwatch supports the latest version of Chrome, Firefox, and Microsoft 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.

Hardware

To view the supported hardware platforms for each system version, refer to the [Hardware and Version Support Matrix](#) on Cisco.com.

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

Flow Sensor 4000

If you have a Flow Sensor 4000 model, you will install a patch after you update the appliance to v7.0.x. Instructions are included in this guide. Review the patch Readme file for details.

This requirement applies only to the FS4000 model. It does not apply to the other models in the Flow Sensor 4000 series.

SMC

You can update a maximum of two SMCs for this update. If you have more than two SMCs, refer to [1. Review Your Cluster](#) for instructions.
UDP Director

If your UDP Directors are configured as a High Availability pair, make sure they aren’t managed by a virtual IP address. Refer to 1. Review Your Cluster for details.

Licensing

Before you start the update, make sure your appliance licenses are up-to-date.

- **Check:** Log in to the SMC Web App. Select the Global Settings icon > Administer Appliance. Select Configuration > Licensing.
- **Status Not Available:** Your secondary SMC licensing status may be displayed as “Status Not Available.” This occurs because of the failover relationship with the primary SMC, but it does not represent the secondary SMC communication status. To see licensing details, click the status button.
- **Guide:** Refer to the Downloading and Licensing Guide for more information.

ISE or ISE-PIC

- **Configuration:** If your SMC uses ISE or ISE-PIC, make sure the Client Group includes Adaptive Network Control (ANC) before you start the update.
- **Check:** Log in to the ISE client. Select Administration > pxGrid Services. Review the SMC > Client Group column. Check each SMC in the list.

  If ANC is not shown, check the SMC check box to select it. Click Group. Add ANC to the Group field. Click Save.

- **Guide:** Refer to the ISE Integration Enhancements for Stealthwatch and the ANC Policy setup instructions for v7.0 details.

Host Name

- **Configuration:** A unique host name is required for each appliance. We cannot update an appliance with the same host name as another appliance.
- **Check:** Log in to the Appliance Administration interface. Select Configuration > Naming and DNS.

Domain Name

- **Configuration:** A fully qualified domain name is required for each appliance. We cannot update an appliance with an empty domain.
- **Check:** Log in to the Appliance Administration interface. Select Configuration > Naming and DNS.

**NTP Server**

- **Configuration:** At least 1 NTP server is required for each appliance in 7.0.
- **Check:** Log in to the Appliance Administration interface. Select Configuration > System Time and NTP.
- **Problematic NTP:** Remove the 130.126.24.53 NTP server if it is in your list of servers. This server is known to be problematic, and it is no longer supported in our default list of NTP servers.

**Time Zone**

All Stealthwatch appliances use Coordinated Universal Time (UTC) in v7.0.x.

- **Configuration:** Before you start the update, make sure your appliances are set to UTC.
- **Check:** Log in to the Appliance Administration interface. Select Configuration > System Time and NTP.
- **Virtual Host Server:** Make sure your virtual host server is set to the correct time.

Make sure the time setting on the virtual host server (where your virtual appliances are installed) is set to the correct time. Otherwise, the appliances may not boot up.

**Custom Certificates**

Stealthwatch supports certificates in PEM format that are encrypted with RSA. If you have custom appliance identity certificates installed on your appliances, make sure they are valid and current before you start the update process. We cannot update appliances with invalid or expired appliance identity certificates.

Review the following options to replace an expired certificate:

- **Update Certificate:** Request an updated certificate from your provider, and install it on the Appliance Administration interface. Select Configuration > SSL Certificate.
- **Restore Default:** Restore the appliance identity certificate default. Log in to the Appliance Administration interface. Select Configuration > SSL. In the SSL Server Identity section, click Restore Defaults.

For instructions, please refer to the [Creating and Installing SSL Certificates Guide](#).
Trust Store

Make sure each appliance identity certificate and certificate chain (if applicable) are saved to the appliance trust store (its own trust store) and the SMC trust store. This configuration is required for all appliances.

- **Configuration:** Before you start the update, make sure the appliance identity certificate and certificate chain (root and intermediate) are saved to the appliance trust store and the SMC trust store.
- **Check:** Log in to the Appliance Administration interface. Select Configuration > Certificate Authority Certificates.

For instructions, please refer to the Creating and Installing SSL Certificates Guide.

⚠️ Make sure you upload your certificates individually to the required Trust Stores.

Backing Up Your Appliances

Make sure you plan time to back up your Stealthwatch system. You’ll need the backup files if there’s a problem with the update, and the diagnostics pack is important for troubleshooting with Cisco Stealthwatch Support.

This guide provides instructions for the following:

- backing up each appliance
- backing up the SMC database
- backing up the Flow Collector database
- creating a diagnostics pack

⚠️ Without a backup, you will not be able to recover your files if a problem occurs during the update process. In addition, the diagnostics pack can be invaluable if you need to troubleshoot with Cisco Stealthwatch Support.

Backing up the Flow Collector Database

The procedure for backing up the Flow Collector database includes trimming the database and deleting snapshots after the backup is finished. Refer to 6. Back Up the Flow Collector and SMC Databases for details.

⚠️ Make sure you follow the instructions and complete all procedures for the database backup. For assistance, please contact Cisco Stealthwatch Support.
Best Time to Update

Consider the following points when you are planning time and resources to update your Stealthwatch appliances.

Software Update Files

It takes time to download the software update files. You can download the files from the Download and License Center in advance.

All Appliances

- **Time:** The update process takes approximately 30 minutes to complete per appliance but may take longer depending on your network. This estimate does not include the time needed to create backups and diagnostic packs, which can also vary depending on your environment.

- **Low Volume:** We recommend that you update the entire system at one time when your system will be experiencing relatively low volumes of traffic.

- **Restart:** Your appliances will reboot automatically after the SMC pre-SWU installation, the Finalize Pre-SWU procedure, and the SWU installation. The appliances do not collect data during the restart process. However, your current data is preserved.

SMCs and Flow Collectors

- **Last Reboot/Active:** Make sure the SMC and Flow Collector have been running for more than one hour but less than seven days before you begin the update process. If they have not, the SWU files will not install due to a migration safety switch.

- **Flow Collectors:** After a Flow Collector is updated and running, it will cache data to be sent to the SMC until the SMC is updated. However, you will not want that process to run for a long time. Preparing all appliances so they can be updated at once is the most successful approach.

> Do not delete any Flow Collectors from the SMC Desktop Client. Doing so will cause the SMC to lose all of the historical data for those Flow Collectors.

Communications

- **Communications:** During the update process, communications will stop between the SMC and the Flow Collectors. When this happens, the Flow Collector icons on the Enterprise tree in the SMC Desktop Client will display a red “x” and the managed appliance icon will be orange (.minecraft) instead of green.
• **Management Channel Down:** If you have any **Stealthwatch Flow Sensors**, you will see a Flow Sensor Management Channel Down alarm on the Alarm Table in the SMC Desktop Client. When the update is complete, communications are re-established, the icons return to normal appearance, and the alarm disappears.
After the Update

Upgrade Issue
After upgrading to v7.0.3, there is a chance the Update Manager will show that your appliance is still on the previous version. You will need to manually reboot the appliance to complete the upgrade.

Patch Installation
After you update your system to v7.0.3, make sure you install any required patches.
Follow the instructions in this guide, and review the patch readme instructions on the Stealthwatch Download and License Center for details.
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):** 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.

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.

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.
Stealthwatch IDentity Appliances (A10)

If you have a Stealthwatch IDentity Appliance (ID-1000, ID-1100), use the following instructions to replace the ID-1000/1100 Lancope web certificate before you update the software to v7.0.x.

If you do not have a Stealthwatch IDentity Appliance in your cluster, you can skip this section and go to Update Overview.

Make sure you follow these instructions to replace the Lancope web certificate before you start the update to version v7.0.x.

1. Update the Software

For increased security, we recommend updating the ID-1000 and ID-1100 so your appliance has the new openSSL version with TLS 1.2.

Please refer to the Upgrade topic in the Stealthwatch IDentity Appliance online help for instructions.

2. Review the Current Certificate

1. Log in to your Stealthwatch IDentity Appliance.
2. Click AAA.

4. Review the list of current certificates. In the Category column, locate the Web certificate that has a green check mark in the Status column.
5. Click the **Certificate** icon.

6. Review the **Issuer** section. If it includes **Lancope** in the description, the certificate needs to be replaced. Proceed to the next section.

3. Create a New Certificate

1. Click **Action > New > Certificate**.

2. Create a new certificate using the following parameters:

   - **Common Name**: Enter a unique name (preferably the fully qualified domain name of the appliance). If you have more than one Stealthwatch IDentity Appliance, make sure you use a unique name for each appliance.
   - **Valid Days**: 1460
   - **Key Length**: 4096
   - **Signature Algorithm**: Select SHA256WithRSA (or a higher SHA).

3. Click **OK**.

4. The appliance restarts automatically.

4. Confirm the New Certificate

Use the following instructions to confirm the new certificate is created and enabled.

1. Log in to your Stealthwatch IDentity Appliance.

2. Click **AAA**.

3. Click **View > Certificate > Web**.
4. Locate the new Web certificate. The common name is listed as **CN= the common name you assigned**.
   - Confirm there is a green check mark in the **Status** column.
   - Note the ID number. You will use it in the next section.

5. Click the **Certificate** icon.
6. Review the new certificate and confirm it shows the following:
   - **Issuer**: Confirm that Lancope is no longer shown in the description. It will most likely show San Jose.
   - **Valid From**: Confirm it shows the date you created the new certificate.
5. Enable the Certificate

After you add the certificate to the Web UI, use the following instructions to enable the certificate in the terminal.

1. SSH in to your Stealthwatch IDentity Appliance.
   
   You may have to reboot your appliance.

2. Type the appliance IP address. Press the Enter key.

3. Type `enable`. Press the Enter key.

4. Enter the appliance password. Press the Enter key.
   
   **Default:** lan911cope

5. Type `config terminal`. Press the Enter key.

6. Type `crypto cert enable web ID`. Press the Enter key.

   **ID:** Enter the certificate ID number that you noted in the previous section.

7. After the OK prompt, type `exit`. Press the Enter key.

   If you do not see the OK response, please contact Cisco Stealthwatch Support.

8. **Log Out:** Type `exit`. Press the Enter key.

6. Verify and Export

1. Log in to your Stealthwatch IDentity Appliance.

2. Click the **Security** icon in the browser address bar.

3. Click **Certificate**.
4. Confirm the new certificate is shown. Make sure it doesn’t show the old, Lancope certificate.
5. Click OK to close the certificates dialog box.
6. Click AAA.
7. Click View > Certificate > Web.
8. Locate the old Lancope certificate. Click the Trash icon to delete it.
9. Locate the new certificate.
10. Click the Export icon. Click OK.
11. The certificate will download. Note the file name and location.
12. Click Cancel to return to the previous page.

7. Install the New Certificate on your SMC

   1. Log in to your SMC.
   2. Click the Global Settings icon.
   3. Select Administer Appliance.
   4. Click Configuration > Certificate Authority Certificates.
   5. In the Certificate Authority Certificates section, click Choose File. Select the new certificate you exported from the IDentity Appliance.
   6. In the Name field, enter the name of the certificate without spaces.
      For example: A10-1100-A.
   7. Click Add Certificate.
   8. Follow the on-screen prompts to confirm the new certificate.
   9. In the Name column of the Certificate Authority Certificates list, locate the ID-1000 or ID-1100 certificate.
      This is the old certificate. The Issued To and Issued By descriptions show Lancope.
10. In the ID-1000 or ID-1100 row, check the **Delete** check box.

> Make sure you select the old ID-1000 or ID-1100 certificate. Do not delete the SMC Lancope appliance identity certificate. Review the screenshot (above) for details.

11. Click **Delete**.
12. Follow the on-screen prompts to confirm.
Update Overview

New Process

Please note that we have a new process for updating appliances from version 6.10.x to v7.0.3 (or a later version of 7.0.x). The new process involves installing pre-SWU and SWU files on your appliances in a specific order.

Make sure you follow the software installation order for both the pre-SWU and SWU files. For a successful update, it is important to follow the steps in this guide.

Update Process Overview

To ensure a successful update and minimize data loss, make sure you follow the instructions in order.

1. Review Your Cluster
2. Confirm the Installed Software Version
3. Download the Patch and Update Files
4. Back Up the Appliance Configuration
5. Create a Diagnostics Pack
6. Back Up the Flow Collector and SMC Databases
7. Check the Available Disk Space
8. Install the Pre-SWU Patch on SMCs using the Appliance Admin.
9. Install the Pre-SWU Patch on Managed Appliances using the System Management page.
10. Finalize the Pre-SWU Installation
11. Install the v7.0.x Software Update. Use the SMC System Management page to update each managed appliance. Make sure you install the v7.0.x SWU using the new order.
12. Log in to Central Management
13. Install v7.0.3 Patches
14. Log in to the SMC Desktop Client: trust the certificate, review failover roles.
15. Update Stand-Alone Appliances and Disconnected Appliances and add stand-alone appliances to Central Management if required.
1. Review Your Cluster

Use the following instructions to review your Stealthwatch appliances.

**Best Practices**

We recommend the following best practices to start the update:

- **SMC Management:** Configure all Stealthwatch appliances so they are managed by your Stealthwatch Management Console (SMC).
- **Stand–Alone Appliances:** If an appliance is not managed by the SMC, it is described as a stand-alone appliance. With the exception of the Endpoint Concentrator, we recommend that you set up all appliances so they are managed by your primary SMC.

If you have a stand-alone appliance, you can update it after the v7.0.x cluster update is completed. See [15. Update Stand–Alone or Disconnected Appliances](#) and [Managed and Stand–Alone Requirements in Central Management](#) for details.

- **Disconnected Appliances:** If you have an appliance that is disconnected during the update process, or if you have appliances associated with your cluster that are not managed by your SMC, you may be prompted to disconnect them from the cluster as part of the update process. You can update the appliance and management configuration after the v7.0.x update is completed. See [15. Update Stand–Alone or Disconnected Appliances](#) and [Managed and Stand–Alone Requirements in Central Management](#) for details.

- **SMC Maximum:** You can update two SMCs for this update.
- **UDP Director High Availability:** If your UDP Directors are configured as a High Availability pair, make sure they aren’t managed by a virtual IP address. Refer to [1. Review Your Managed Appliances](#) for details.

Once you start the update process, do not add or remove appliances, change your cluster configuration, or change the appliance failover roles. You can add these appliances to your cluster after the 7.0.x update.
1. Review Your Managed Appliances

Review the appliances in your Stealthwatch cluster by checking the SMC System Management list. Use this procedure to make any final changes to your Stealthwatch cluster before you start the update.

1. Log in to your primary SMC Web App. (https://[IP address]).
2. Click the **Global Settings** icon. Select **System Management**.

3. Review the appliances listed in the System Visibility section.

   - **Missing Appliances:** To add appliances to this list so they are managed by the SMC, go to **Add Appliances to Your Stealthwatch Cluster**.
   - **Outdated Appliances:** To remove appliances from SMC System Management, or if the time in the **Device Last Seen** column is not up to date, go to **Remove Appliances from Your Stealthwatch Cluster**.
   - **UDP Director High Availability:** If your UDP Directors are configured as a High Availability pair, make sure they aren't managed by a virtual IP address. If you have a UDP Director virtual IP address in the list, remove it using **Remove Appliances from Your Stealthwatch Cluster**.
Add Appliances to Your Stealthwatch Cluster

Use the following steps to add an appliance to your Stealthwatch cluster so it is managed by the SMC. With the exception of the Endpoint Concentrator, we recommend that you set up all appliances so they are managed by your primary SMC.

Although having all appliances managed by the SMC is the fastest way to update your appliances, this step is not required. You can update stand-alone appliances after the v7.0.x update is completed. Refer to 15. Update Stand-Alone or Disconnected Appliances and Managed and Stand-Alone Requirements in Central Management for details.

1. Log in to the Appliance Admin interface.
3. Uncheck the Accept connections from any management system check box.
4. Check the List: Review the Management System Configuration list. Delete any SMCs that are not active in your system.
5. Click Add New Management System.
6. Enter the primary SMC IP address and any other required fields. Repeat step 5 if you have a secondary SMC (failover only).
7. Click Apply. Follow the on-screen prompts.
8. Return to the SMC System Management page. Confirm the appliance is listed. You may have to refresh the page.

Remove Appliances from Your Stealthwatch Cluster

Use the following steps to remove an appliance from your Stealthwatch cluster so it is not managed by the SMC.
1. Log in to the Appliance Admin interface.
2. Select **Configuration > Management Systems Configuration**.
3. Uncheck the **Accept connections from any management system** check box.
4. Locate the SMC in the management list.
5. Check the **Delete** check box.
6. Click **Apply**. Follow the on-screen prompts.
7. Log in to the SMC Appliance Admin interface.
   - On the SMC System Management page, click the **Global Settings** icon.
   - Select **Administer Appliance**.
8. Select the **Home** page.
9. In the Services section, click **Reload** on the following services:
   - upserv_uwsgi
   - authserv_uwsgi
10. Return to the SMC System Management page. Confirm the appliance is removed. You may have to refresh the page.

   **If the appliance is not removed**, log in to the SMC Desktop Client and delete the appliance from the Enterprise tree.
   - Right click the appliance.
   - Select **Configuration > Delete**.

2. Check Flow Sensor Settings

Use the following instructions to review the management channels and traffic settings on your Flow Sensors.

1. Log in to the Flow Sensor Appliance Admin interface.
2. Select **Configuration > Management Systems Configuration**.
3. Review the Management System Configuration list.
   - **If the Flow Sensor is managed by your SMC**, confirm your primary SMC and secondary SMC (if used) are shown in this list. If you have more than two
SMCs shown, delete the inactive SMCs.

- **If the Flow Sensor is not managed by the SMC**, make sure this list is empty. If there are SMCs in this list, delete them.

4. Select **Configuration > Net Flow Collectors**.
5. Review the NetFlow Collectors list.

- Confirm the Flow Collectors in the list should be receiving traffic from the Flow Sensor.
- Delete any inactive or extra Flow Collectors.

Once you start the update process, do not add or remove appliances, change your cluster configuration, or change the appliance failover roles. You can add these appliances to your cluster after the 7.0.x update.
2. Confirm the Installed Software Version

Complete these steps to verify that the current software version for each appliance is **6.10.2, 6.10.3, or a later version of 6.10.x**. Also, make sure all appliances are using the same software version. For example, if your SMC has v6.10.3 installed, the other appliances in your cluster need v6.10.3 installed.

1. Go to your SMC Web App dashboard.
2. Click the **Global Settings** icon. Select **System Management**.

![Global Settings Icon](image)

3. Review the **Installed Version** column. Confirm each appliance has v6.10.2 or 6.10.3 (or later) installed.

**Same Version:** Make sure all appliances are using the same software version. For example, if your SMC has v6.10.3 installed, the other appliances in your cluster need to have v6.10.3 installed.

![Installed Version](image)

Also, review the additional notes for each version below.
• **6.9.x or earlier:** If the installed version is 6.9.x or earlier, update the appliance to v6.10.4 (or the latest version of 6.10.x) using the [Stealthwatch Update Guide on Cisco.com](https://www.cisco.com).

• **6.10.2:** If the installed version is 6.10.2, install the 6.10.2 rollup patch using the instructions in the Readme file. `patch-smc-ROLLUP008-6.10.2-01.swu (or later)` is required for this update. Log in to [https://stealthwatch.flexnetoperations.com](https://stealthwatch.flexnetoperations.com) for details.

• **6.10.3** If the installed version is 6.10.3, install the 6.10.3 rollup patch using the instructions in the Readme file. Log in to [https://stealthwatch.flexnetoperations.com](https://stealthwatch.flexnetoperations.com) for details.

• **6.10.4:** If the installed version is 6.10.4, install the 6.10.4 rollup patch using the instructions in the Readme file. `patch-common-lc-admin-6.10.4-01.swu (or later)` is required for this update. Log in to [https://stealthwatch.flexnetoperations.com](https://stealthwatch.flexnetoperations.com) for details.

• **6.10.x** If the installed version is 6.10.5 or later, make sure you install the latest rollup patch using the instructions in the Readme file. Log in to [https://stealthwatch.flexnetoperations.com](https://stealthwatch.flexnetoperations.com) for details.

⚠️ Make sure every appliance has the correct software version installed. This step is critical for a successful update.
3. Download the Patches and Update Files

Use the following instructions to download the pre-SWU and v7.0.x update SWUs.


2. Log in to the Download and License Center.

3. Select **Downloads > Upgrade Stealthwatch**.

4. On the Current Versions tab, click the appliance name. Click the software release link to download it (or select FTP Download).

   - Each appliance has one unified update file for both the virtual (VE) and physical appliance.
   - Download the patch pre-SWU and update (SWU) files for all of your appliances. Refer to the **SWU Files** chart for details.
   - **Details**: Click the down arrow next to each item to see additional software information.

---

Download and install the appliance software update files individually. Due to file size and web application limitations, we do not recommend zipping or bundling the software update files.
### Pre-SWU (Patch) Files

<table>
<thead>
<tr>
<th>Appliance</th>
<th>Patch File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMC</td>
<td>patch-smc-pre-7.0-jumpstart-PATCH1-01.swu</td>
</tr>
<tr>
<td>All Other Appliances</td>
<td></td>
</tr>
<tr>
<td>• Flow Collector</td>
<td>patch-common-pre-7.0-jumpstart-PATCH1-01.swu</td>
</tr>
<tr>
<td>• Flow Sensor</td>
<td></td>
</tr>
<tr>
<td>• UDP Director (also known as FlowReplicators)</td>
<td><strong>Download Once:</strong> You will use this one file to update each appliance.</td>
</tr>
<tr>
<td>• Endpoint Concentrators</td>
<td></td>
</tr>
</tbody>
</table>

### SWU Files

<table>
<thead>
<tr>
<th>Appliance</th>
<th>Update File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP Director</td>
<td>update-udp-7.0.3.2020.03.16.1824-01.swu</td>
</tr>
<tr>
<td>UDP Director VE</td>
<td>update-udp-7.0.3.2020.03.16.1824-01.swu</td>
</tr>
<tr>
<td>Flow Collector 5000 series Database</td>
<td>update-fcdb-7.0.3.2020.03.16.1826-01.swu</td>
</tr>
<tr>
<td>Flow Collector for NetFlow</td>
<td>update-fcnf-7.0.3.2020.03.16.1827-01.swu</td>
</tr>
<tr>
<td>Flow Collector for sFlow</td>
<td>update-fcsf-7.0.3.2020.03.16.1827-01.swu</td>
</tr>
<tr>
<td>Endpoint Concentrator</td>
<td>update-ec-7.0.3.2020.03.16.1824-01.swu</td>
</tr>
<tr>
<td>Appliance</td>
<td>Update File Name</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>SMC and SMC VE</td>
<td>update-smc-7.0.3.2020.03.16.1829-01.swu</td>
</tr>
<tr>
<td>Flow Sensor Appliance</td>
<td></td>
</tr>
<tr>
<td>Flow Sensor VE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>update-fsf-7.0.3.2020.03.16.1907-01.swu</td>
</tr>
</tbody>
</table>
4. Back Up the Appliance Configuration

Complete these steps to back up each appliance configuration. These steps are important to help minimize data loss.

⚠️ Without a backup, you will not be able to recover your files if a problem occurs during the update process.

1. Log in to the Appliance Admin interface as the admin user.
2. Select the Home page.
3. Review the IP address and host name. Verify that this is the appliance you want to update.
4. Click **Support > Backup/Restore Configuration**.
5. Under the Backup section, click **Create Backup**.

6. When the backup process is finished, click **Download**. Save the backup (TGZ) file to your preferred location.

7. Click **Close** to close the progress window.
8. Repeat steps 1 to 7 on every appliance.
5. Create a Diagnostics Pack

Having a diagnostics pack can be invaluable if you need to work with Cisco Stealthwatch Support to troubleshoot an issue.

To create a diagnostics pack using Appliance Administration, complete the following steps:

1. Click Support > Diagnostics Pack.
2. Click Create Diagnostics Pack.
3. Click Download and save the diagnostics pack (GPG) file to your preferred location. This process may take a few minutes.
4. Click Close to close the progress window.

**Time-Out:** 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 diagnostics pack without timing out. The diagnostics pack is located in `/lancope/var/admin/diagnostics`. 
6. Back Up the Flow Collector and SMC Databases

After creating a diagnostics pack for a Flow Collector or SMC, back up the Flow Collector and SMC databases.

If the appliance is not a Flow Collector or SMC, you can skip this procedure.

This process involves completing the following procedures:

1. **Disable SNMP polling.**
2. **Trim the Flow Collector database.**
3. **Back up the databases.**
4. **Delete the Flow Collector snapshots.**
5. **Re-enable SNMP polling.**

Without a backup, you will not be able to recover your files if a problem occurs during the update process.

1. **Disable SNMP Polling for an SMC**

Backing up the database can take a long time. To prevent the SNMP process from interrupting the backup, turn off SNMP polling. Then, re-enable SNMP polling after the backup finishes.

To disable SNMP polling, complete the following steps.

1. Launch the SMC Desktop Client as the admin user (but do not close the Appliance Admin interface).
2. In the Enterprise tree, right-click an exporter.
3. **Select Configuration > Exporter SNMP Configuration.**
4. Note the entry in the **Default** field. You will re-enter this information after you back up the databases.
5. In the **Default** drop-down list, select **None**. SNMP polling for this domain is now off.

6. Click **OK**.

7. Repeat steps 2 to 5 for each domain on your system.

---

2. **Trim the Flow Collector Database**

The Flow Collector database backup may take multiple days to finish and will slow your network speed if the database is large. Before you back up your databases, we recommend trimming the Flow Collector database. This will free the available disk space for storing flows and reduce the amount of time it takes to back up the database.

The Flow Collector stores the maximum number of days based on the disk space and the amount of data collected per day. When the maximum (75% of the /var partition) is hit, the database will start to delete the oldest data first to allow new data to come in.

---

1. **Review your Database Storage Statistics**

Use the following instructions to check your database storage.

1. Log in to the Flow Collector Appliance Admin interface.

2. Select **Support > Database Storage Statistics**.

3. Review the days stored in Capacity, Flow Data Summary, and CI Event Data Summary.
2. Trim the Interface Details

The Flow Interface Data is the data related to the interfaces of exporters. Stealthwatch saves flow interface data and flow data. The Flow Interface default setting causes the system to push out the flow data, so it can keep all the interface statistics it can.

We recommend changing the Flow Interface Data Storage limit to 15 or 30 days. In this configuration, any data older than the limit will be lost.

Use the following instructions to purge the database of the interface statistics data older than 15 or 30 days, so you can free up the available disk space for storing flows.
1. Log in to your Stealthwatch Desktop Client as the admin user.
2. Locate the Flow Collector in the Enterprise Tree. Click the plus (+) sign to expand the container.
4. In the Flow Collector Properties dialog box, click Advanced.
5. Select the Store flow interface data field. Set the limit to Up to 15 days or 30 days.
6. Click OK.

3. Trim Flow Details and CI Event Data

To reduce the size of the Flow Details & CI Event/Details in the Flow Collector database, please contact Cisco Stealthwatch Support. This step is optional, and the trimming process takes only a few minutes to complete, but the process requires guidance.

When you trim the NetFlow, you will specify the number of days to keep Flow Details & CI Event/Details in the Flow Collector database. Two things will occur with this configuration:

- The database is trimmed down to the number of days you enter.
- The database starts rolling the older data out based on the oldest day but without trying to save as much as possible.

3. Back Up the Databases

To back up a Flow Collector or SMC database to a remote file system, complete the following steps.

- **Space:** Make sure the remote file system has enough space to store the database backup.
- **Time:** After you back up the database once, subsequent backups will be quicker because the process backs up only what has changed since the last backup. This process backs up approximately 0.5 GB to 2 GB of data per minute.

1. Return to the Appliance Admin interface (but do not close the SMC Desktop Client).
2. Determine how much space you will need on the remote file system to store the database backup as follows:
   - Click Home.
   - Locate the Disk Usage section.
Review the **Used (byte)** column for the `/lancope/var` file system. You will need at least this much space plus 15% more on the remote file system to store the database backup.

3. Click **Configuration > Remote File System**.

4. Complete the fields using the settings for the remote file system where you want to store the backup files.

   The Stealthwatch file share uses the CIFS (Common Internet File System) protocol, also known as SMB (Server Message Block).

5. Click **Apply** to place the settings in the configuration file.

   If the Apply button is not enabled after you enter the password, click once in a blank area on the Remote File System page to enable it.

6. Click **Test** to verify that the Stealthwatch appliance and the remote file system can communicate with each other.

   You should see the following message at the bottom of the Remote File System page when the test is complete.
7. Click **Support > Backup/Restore Database**. The Backup Database page opens as shown in the following example.

![Backup Database](image)

8. Click **Create Backup**. This process may take a long time.

   - After the backup process starts, you can mouse away from the page without interrupting the process. However, if you click Cancel while the backup is in progress, you may not be able to resume the backup without restarting the appliance.
   - Follow the on-screen prompts until the backup is completed.
   - To view details of the backup process, click View Log.

![Backup Status](image)

9. Click **Close** to close the progress window.
4. Delete the Flow Collector Snapshots

After you have saved the backup files, use the following instructions to delete the snapshots.

> Make sure you delete the Flow Collector snapshots. This step is critical for a successful update.

1. SSH in to the Flow Collector.
2. Log in as admin.
3. **Check for Snapshots:** Type:

   ```
   /opt/vertica/bin/vsql -U dbadmin -w lan1cope -c "select * from database_snapshots;"
   ```

4. **Delete Snapshots:** Type:

   ```
   /opt/vertica/bin/vsql p5433 -U dbadmin -X -q -c "select remove_database_snapshot('StealthwatchSnap1');"
   ```

5. Repeat these steps to delete all saved Flow Collector database snapshots.

5. Re-enable SNMP Polling in the SMC

To re-enable SNMP polling, complete the following steps.

1. Return to the SMC Desktop Client (but do not close the Appliance Admin interface).
2. Right-click the appropriate domain and select **Configuration > Exporter SNMP Configuration.** The Exporter SNMP Configuration page for that domain opens.
3. From the Default drop-down list, select the original entry for the selected domain (refer to step 3 in Disable SNMP Polling). SNMP polling for this domain is now re-enabled.
4. Click **OK.**
5. Repeat steps 2 to 4 in this procedure for each domain on your system.
6. Close the SMC Desktop Client.
7. Check the Available Disk Space

Check the disk space on each appliance to confirm you have enough disk space for the software update.

1. Log in to the Appliance Admin interface.
2. Click Home.
3. Locate the Disk Usage section.
4. Review the Available (byte) column and confirm that you have at least 4 times the size of the software update file (SWU) free on the /lancope/var/ partition.
   - For example, if the software update file (from the Download and License Center) is 6 GB, you should have 24 GB available on the partition.
   - When the SWU is uploaded to the SMC, it will use additional space during the update. Once the update is completed, the SWU will be removed from the file system.

<table>
<thead>
<tr>
<th>Disk Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>/</td>
</tr>
<tr>
<td>lancope/var</td>
</tr>
</tbody>
</table>

5. If you need to expand the appliance disk space, see the Data Storage section of the Stealthwatch Installation and Configuration Guide for your appliance.
8. Install the Pre-SWU Patch on SMCs

Use the following instructions to install the Pre-SWU patch on your Stealthwatch Management Console (SMC) using the Appliance Admin interface.

If you have an SMC failover pair, make sure you install the pre-SWU on your secondary SMC first.

⚠️ Once you start the update process, do not add or remove appliances, change your cluster configuration, or change the appliance failover roles. You can add these appliances to your cluster after the 7.0.x cluster update.

1. Log in to your SMC as the administrator (https://[IP address]).

   If you have an SMC failover pair, log in to the secondary SMC first.

2. Click the Global Settings icon. Select Administer Appliance.

3. Click Support > Update.

4. Click Choose File.

5. Select the patch pre-SWU file:

   patch-smc-pre-7.0-jumpstart-PATCH1-01.swu

6. Click Open.

7. Check the Automatically Execute check box.

8. Click Upload. Follow the on-screen prompts to start the installation.

9. When the Update Progress is shown as complete and rebooting, refresh the page.

© 2020 Cisco Systems, Inc. and/or its affiliates. All rights reserved.
This may take more time than a typical patch.

**Reboot**: The system reboots automatically.

**Refresh**: While the appliances and services restart, the page might pause. Refresh the page to see the progress.

10. **Confirm Installation**: Log in to the SMC Appliance Admin interface.

   - Select **Support > Update**.
   - In the **Last Update Status** section, confirm the pre-SWU is shown as successfully applied. Click **View Log** for details.


11. If you have an SMC failover pair, repeat procedure **8. Install the Pre-SWU Patch on SMCs** to install the pre-SWU patch on the primary SMC.
9. Install the Pre-SWU Patch on Managed Appliances

Once you’ve installed the pre-SWU patch on your primary SMC Appliance Admin, it will prepare your managed appliances for the pre-SWU installation on the System Management page. Use these instructions to install the pre-SWU patch on your managed appliances.

1. Go to your primary SMC Web App dashboard.
2. Click the **Global Settings** icon. Select **System Management**.
3. In System Visibility, review your appliance list.
   - Confirm the pre-swu patch-common-pre-7.0-jumpstart-PATCH1-01.swu is listed for each appliance in the **Version Ready to Install** column.
   - **SMC**: The Version Ready to Install for the SMC will be blank because you already installed it.

4. Take a screenshot of your System Visibility list to use as a reference.
5. Click the **Actions** menu for the appliance. Select **Install Update**.
   - **Order**: You can install the pre-SWU on the appliances in any order as long as you’ve updated your SMCs first.
   - **Multiple Appliances**: You can install the pre-SWU on multiple appliances at the same time.
   - **Status**: Check the **Update Status** column and refresh the page to see the update progress.

6. Repeat step 5 on every appliance in System Visibility.
7. Check the **Update Status** column. Confirm **Patch Applied** is shown for every appliance (except the SMCs).
9. Install the Pre-SWU Patch on Managed Appliances

<table>
<thead>
<tr>
<th>Host Name</th>
<th>Device IP</th>
<th>Device Last Seen</th>
<th>Device Model</th>
<th>Installed Version</th>
<th>Version Ready to Install</th>
<th>License Status</th>
<th>Upgrade Status</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>flow</td>
<td>10.0.0.1</td>
<td>12:29 PM 8/1/2018</td>
<td>StealthWatch FlowCollector for NetFlow VE</td>
<td>6.10.2.2018.06.01.1035-0</td>
<td>90 Days on Line</td>
<td></td>
<td>Patch applied 0:30 PM 6/3/2018</td>
<td></td>
</tr>
<tr>
<td>smu</td>
<td>15.0.0.1</td>
<td>12:29 PM 8/1/2018</td>
<td>StealthWatch Management Console VE</td>
<td>6.10.2.2018.06.01.1041-0</td>
<td>90 Days on Line</td>
<td></td>
<td>Patch applied 0:30 PM 6/3/2018</td>
<td></td>
</tr>
<tr>
<td>te</td>
<td>10.0.0.1</td>
<td>12:29 PM 8/1/2018</td>
<td>StealthWatch FlowSensor VE</td>
<td>6.10.2.2018.06.01.1035-0</td>
<td>90 Days on Line</td>
<td></td>
<td>Patch applied 0:30 PM 6/3/2018</td>
<td></td>
</tr>
</tbody>
</table>
10. Finalize the Pre-SWU Installation

Use the following instructions to finalize your cluster with the pre-SWU installation and prepare it for the v7.0.3 upgrade.

Once you finalize the pre-SWU installation, we recommend that you upgrade your appliances as soon as possible. You can use your appliances in between the pre-SWU and v7.0.x SWU update, but functionality is limited.

1. Click Check Pre-SWU Status and Finalize.
2. Review the **Disconnect From Cluster List**.

If there are not appliances in the Disconnect list, go to step 3.

If there are appliances in the Disconnect list, the pre-SWU has not finished installing on those appliances.

- Click **Refresh** as needed, and wait until the appliances move to the **Finalize With Cluster** list.

- Review the following options to determine if you need to keep the appliances in your Stealthwatch cluster or if you want to disconnect them:

<table>
<thead>
<tr>
<th>Option</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keep in Cluster</td>
<td>To keep these appliances with your Stealthwatch cluster, click <strong>Refresh</strong> as needed, and wait until they...</td>
</tr>
</tbody>
</table>
To disconnect these appliances from your Stealthwatch cluster, and skip the pre-SWU installation on them, go to step 3.

**If you disconnect appliances:**

- They won’t update to the next version with the rest of your cluster.
- You will lose the connection to them.
- You can add appliances to your cluster later, but you will update them separately.
- Take a screenshot of the list so you don’t lose the IP addresses.

If the appliances in the Disconnect From Cluster list should be updated with your cluster, but they are not progressing to the Finalize With Cluster list, click **Cancel**. Contact [Cisco Stealthwatch Support](https://www.cisco.com/c/en/us/support/security/cisco-stealthwatch-systems/technical-support.html) for assistance.

**Port Warning:** Your appliances use **port 5672** to communicate for this update. For details, refer to **Port 5672**. If you encounter port errors during the update, make sure this port is open, or contact your system administrator.

**SMC Failover:** If the SMC failover configuration fails, or if you lose one of the SMCs in your failover pair, contact [Cisco Stealthwatch Support](https://www.cisco.com/c/en/us/support/security/cisco-stealthwatch-systems/technical-support.html) for assistance.

3. Confirm all appliances in your cluster are listed in the **Finalize With Cluster** section. If they are, you are ready to finalize the pre-SWU installation and move forward with the update.
If you click Finalize, the appliances listed in Disconnect From Cluster list are disconnected and removed from your Stealthwatch cluster. You can update these appliances separately.

4. Click **Finalize**.

   **Reboot:** The system reboots automatically.

   **Refresh:** While the appliances and services restart, the page might pause. Click **Refresh** to see the progress of the pre-SWU Finalize process.

5. When the Finalize Status shows **Rebooting**, click **Close**.
6. On the System Management page, an error displays that the server is offline. Refresh the page.

7. Log in to your primary SMC Web App (https://[IP address]).

8. Return to the System Management page.
   - Click the **Global Settings** icon.
   - Select **System Management**.

9. Click **Check Pre-Swu Status and Finalize**.

   **Complete:** Confirm the **Finalize Status** is shown as completed.
Incomplete: If the Finalize Status is not complete, return to the System Management page. Check the status of the pre-SWU installation or contact Cisco Stealthwatch Support.

⚠️ If the pre-SWU installation failed on the SMC, do not try the installation again. Please contact Cisco Stealthwatch Support.
11. Install the 7.0 Software Update

You will continue using the System Management page for the 7.0.3 (or a later version of 7.0.x) software update.

⚠️ Make sure your SMCs and Flow Collectors have been running for more than one hour before you start the v7.0.x software update.

Use the New Update Order

Update your appliances in the following order:

<table>
<thead>
<tr>
<th>Order</th>
<th>Appliance</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>UDP Directors (also known as FlowReplicators)</td>
<td>If you have a High Availability cluster, update the secondary UDP Director first. Confirm the update is installed and the secondary UDP Director is running again before you update the primary UDP Director.</td>
</tr>
<tr>
<td>2.</td>
<td>Flow Collector 5000 Series Database</td>
<td>Make sure the Flow Collector has been running for more than one hour before you start the update.</td>
</tr>
<tr>
<td>3.</td>
<td>Flow Collector 5000 Series Engine</td>
<td>Make sure the Flow Collector 5000 series database completes the update and is running again before you start the engine update.</td>
</tr>
<tr>
<td>4.</td>
<td>All Other Flow Collectors (NetFlow and sFlow)</td>
<td>Make sure the Flow Collector has been running for more than one hour before you start the update.</td>
</tr>
<tr>
<td>5.</td>
<td>Flow Sensors</td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td>Secondary SMC (if used)</td>
<td>Make sure the SMC has been running for more than one hour before you start the update.</td>
</tr>
</tbody>
</table>
If your system uses a secondary SMC, confirm the secondary SMC update is installed and confirm the secondary SMC is running again before you start the primary SMC update.

After the update completes, both SMCs may restart in the secondary role. If this occurs, see **Verify SMC Failover Roles** for details. Do not change the failover roles until both SMCs are updated.

### 7. Primary SMC

Make sure the SMC has been running for more than one hour before you start the update.

If your system uses a secondary SMC, confirm the secondary SMC update is installed and confirm the secondary SMC is running again before you start the primary SMC update.

After the update completes, both SMCs may restart in the secondary role. If this occurs, see **Verify SMC Failover Roles** for details. Do not change the failover roles until both SMCs are updated.

### 8. Stand-Alone Appliances and Disconnected Appliances

**Examples:** Endpoint Concentrator or any appliance not managed by the SMC.

**Notes:** Update these appliances after you finish updating all managed appliances. You will update your stand-alone appliances using the **Appliance Admin interface**.
Best Practices

- **Order:** Make sure you update the appliances in order and review the details in the appliance update order before you start.

- **Wait:** Make sure your SMCs and Flow Collectors have been running for more than one hour before you start the v7.0.x software update.

- **Confirm:** Confirm the update is installed and that each appliance is running before you start the next appliance update.

- **Multiple Appliances:** With the exception of SMCs and Flow Collector 5000 series, you can update multiple appliances at the same time as long as they are the same appliance type and you follow the appliance update order and notes.

For example, if you have several Flow Sensors in your cluster, you can update all Flow Sensors at the same time. However, make sure you have completed updating all the Flow Collectors in your cluster first.

**Install the v7.0.3 Update on Managed Appliances**

Use these instructions to install the v7.0.3 software (or a later version of 7.0.x) on appliances managed by the SMC using the System Management page.

1. Log in to your primary SMC Web App (https://[IP address]).
2. Click the **Global Settings** icon. Select **System Management**.

In the System Visibility section, the **Installed Version** column will continue to show v6.10.x installed.
3. **Click Upload an Update File.**

   - **Select File:** Select the v7.0.3 software update file (SWU) that you downloaded from the Download and License Center.
   - **Repeat this step** to upload the v7.0.3 SWU file for each appliance. See the SWU Files chart for details.

4. Review your appliance list in the System Visibility section. Confirm the v7.0.3 software version is shown in the **Version Ready to Install** column.

5. Using the appliance update order, click the **Actions** menu for the appliance. Select **Install Update**.
Make sure you update the appliances in order and review the details in the appliance update order before you start. Confirm the update is installed and that each appliance is running before you start the next appliance update. Refer to steps 6 and 7 to confirm this information.

6. In the System Visibility section, review the Installed Version column. Confirm the appliance has v7.0.3 installed.

   **Refresh:** While the appliances and services restart, the page might pause. Refresh the page to see the current Update Status.


   - **Log In:** Log in to the Appliance Admin interface as the admin user.
   - **Success:** In the Last Update Status section, confirm the update has been successfully installed or applied.
   - **Uptime:** Click Home. Locate the Uptime section. Make sure the appliance is running. The Uptime refreshes every 60 seconds.

8. Repeat steps 5 through 7 for all appliances shown on the System Management page.

   **Reload:** If you have trouble loading any of the pages, clear your browser cache, close and re-open your browser, and log in again.

9. When you update your primary SMC, which is last in the appliance update order, the system reboots. When you log in again, the new Central Management Update Manager page opens.
12. Log in to Central Management

When you update the appliance software to v7.0.x, Central Management is added to your primary SMC.

- **About Central Management:** When your appliances are managed by Central Management, you can review their status and manage the following: edit appliance configuration, update software, reboot, shut down, and more.

- **Stealthwatch Help:** For more information on each page, click the Help icon. Select Stealthwatch Online Help.

1. The last procedure ([Install the v7.0.3 Update on Managed Appliances](#)) brings you to the Central Management Update Manager. Click the **Appliance Manager** tab.

**If you need to log in:**

- Log in to the SMC Web App.
- Click the **Global Settings** icon.
- Select **Central Management**.

2. Review the appliances on the Appliance Manager Dashboard.

- **Managed Appliances:** Confirm that all appliances in your Stealthwatch cluster are listed. Review the **Appliance Status** column and confirm each appliance is shown as **Up**.

- **SMCs:** If you have a primary SMC and secondary SMC, confirm the Appliance Status for each SMC is shown as **Up**.
3. **Root Partition**: Repeat this step on every appliance to check the root partition.

   - Click the **Actions** menu for the appliance.
   - Select **View Appliance Statistics**.
   - Log in to the Appliance Administration interface.
   - On the **Home** page, locate the **Disk Usage** section.
   - 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.
13. Install v7.0.3 Patches

1. Flow Sensor 4000: If you have a Flow Sensor 4000, use the Update Manager page in Central Management to install the required patch.
   - Review the patch readme for details.
   - This requirement applies only to the FS4000 model. It does not apply to the other models in the Flow Sensor 4000 series.
   - For details, log in to the Stealthwatch Download and License Center at https://stealthwatch.flexnetoperations.com.

2. If you use the SMC Desktop Client or an SMC failover pair, continue to the next procedure 14. Log in to the SMC Desktop Client.
   - If you do not use the SMC Desktop Client or an SMC failover pair, you are finished with the v7.0.x upgrade on managed appliances.
   - To update stand-alone appliances, refer to 15. Update Stand-Alone or Disconnected Appliances.
   - To add disconnected or stand-alone appliances to Central Management, refer to 15. Update Stand-Alone or Disconnected Appliances.
14. Log in to the SMC Desktop Client

If you don’t use the SMC Desktop Client or SMC failover configuration, you can skip this procedure. For the list of SMC Desktop Client product capabilities, refer to the Java section of Before you Begin.

Trust the Certificate in the SMC Desktop Client

As part of the v7.0.x update, the default appliance identity certificate (previously Lancope) is replaced with a new, unique, self-signed appliance identity certificate. Use the following instructions to accept the certificate in the SMC Desktop Client.

- If the appliance uses a custom certificate, it will not be replaced. However, you may need to open the SMC Desktop Client and confirm the certificate.
- If you cannot log in to the Desktop Client, confirm you have the correct version of Java installed.

1. Log in to the SMC Web App.
2. Click Desktop Client.
3. Follow the on-screen prompts to review the new certificate and trust it.

If you are not prompted to trust a new certificate, and if you can access your data in the SMC Desktop Client, no further action is required.

Verify SMC Failover Roles

- Do not change the failover roles until both SMCs are updated.
- Do not add or remove appliances from Central Management until you’ve finished the failover configuration and confirmed the secondary SMC Appliance Status is shown as Up in Central Management.

Use the following instructions to confirm your primary SMC and secondary SMC retained their roles after the update.

1. Using an admin-level user name and password, log into the secondary SMC.
2. Open the Desktop Client.
3. In the Enterprise tree, review each branch that displays SMC Failover (Primary) and SMC (Secondary).
4. If both SMCs are shown as secondary, change the failover roles so you have one primary SMC and one secondary SMC. Make sure you follow the instructions in the SMC Desktop Client Help.

For instructions, refer to the SMC Desktop Client Help.

5. Log in to the secondary SMC Web App.
6. Review the Flow Collection Trend.

7. If flow collection is in progress, no further action is required. Go to the next step.

If flow collection stopped, use Central Management to reboot your Flow Collectors and secondary SMC.

- Log in to the primary SMC.
- Open Central Management.
- On the Appliance Manager page, locate the Flow Collector.
- Click the Actions Menu.
- Select Reboot Appliance. Follow the on-screen prompts.
- Flow Collectors: Repeat these steps to reboot every Flow Collector in Central Management.
- Secondary SMC: Repeat these steps to reboot your secondary SMC.

8. Log in to the primary SMC.
9. Review the Central Management > Appliance Manager. Confirm the secondary SMC Appliance Status is shown as Up.
15. Update Stand-Alone or Disconnected Appliances

Use the following instructions to update appliances to v7.0.3 (or a later version of 7.0.x) that have the following scenarios:

- if the appliance is an **Endpoint Concentrator**
- if you **disconnected an appliance** from your cluster during the **pre-SWU installation**
- if you have **stand-alone appliances** that were not updated with the rest of your cluster because they are not managed by an SMC

With the exception of the Endpoint Concentrator, we recommend that you set up all appliances so they are managed by your primary SMC. Please refer to **Managed and Stand-Alone Requirements in Central Management** to determine if you need to add an appliance to Central Management after the update is completed.

If you do not have any disconnected or stand-alone appliances, you are finished with the v7.0.x Stealthwatch update.

1. Check the Software Version

1. Log in to the Appliance Admin interface ([https://[IP address]]). Review the software version shown on the Home page.

- **6.9.x or earlier**: If the installed version is 6.9.x or earlier, update the appliance to v6.10.4 (or the latest version of 6.10.x) using the [Stealthwatch Update Guide on Cisco.com](https://www.cisco.com/c/en/us/products/service-protection-stealthwatch/stealthwatch-update-guide.html).
- **6.10.2**: If the installed version is 6.10.2, install the 6.10.2 rollup patch using the instructions in the Readme file. **patch-smc-ROLLUP008-6.10.2-01.swu (or later)** is required for this update. Log in to [https://stealthwatch.flexnetoperations.com](https://stealthwatch.flexnetoperations.com) for details.
- **6.10.3** If the installed version is 6.10.3, install the 6.10.3 rollup patch using the instructions in the Readme file. Log in to [https://stealthwatch.flexnetoperations.com](https://stealthwatch.flexnetoperations.com) for details.
- **6.10.4**: If the installed version is 6.10.4, install the 6.10.4 rollup patch using the instructions in the Readme file. **patch-common-lc-admin-6.10.4-01.swu (or**
Later) is required for this update. Log in to https://stealth-watch.flexnetoperations.com for details.

- 6.10.x If the installed version is 6.10.5 or later, make sure you install the latest roll-up patch using the instructions in the Readme file. Log in to https://stealth-watch.flexnetoperations.com for details.

Make sure all appliances are using the same software version. For example, if your SMC has v6.10.3 installed, your stand-alone appliance needs to have v6.10.3 installed.

2. Prepare the Appliance

Use the previous procedures in this guide to prepare your appliance for the update. These instructions are important to ensure a successful update and minimize data loss.

- 3. Download the Patches and Update Files
- 4. Back Up the Appliance Configuration
- 5. Create a Diagnostics Pack
- 6. Back Up the Flow Collector and SMC Databases
- 7. Check the Available Disk Space

3. Install the Pre-SWU

1. Click Support > Update.
2. Click Choose File.
3. Select the patch pre-SWU file: patch-common-pre-7.0-jumpstart-PATCH1-01.swu

SMC: If you are updating a stand-alone SMC, select patch-smc-pre-7.0-jumpstart-PATCH1-01.swu.

4. Check the Automatically Execute check box.
5. Click Upload. Follow the on-screen prompts to start the installation.
6. When the Update Progress is shown as **complete** and **rebooting**, refresh the page.

7. Log in to the Appliance Admin interface.
8. Select **Support > Update**.

   - In the **Last Update Status** section, confirm the pre-SWU is shown as successfully applied. Click **View Log** for details.
   - **Reload**: If you have trouble loading any of the pages, clear your browser cache, close and re-open your browser, and log in again.
   - **Log**: Click View Log.

---

If the pre-SWU installation failed, do not try the installation again. Please contact [Cisco Stealthwatch Support](mailto:support@cisco.com).
4. Install the v7.0.x SWU

2. Select the v7.0.x SWU update file for the appliance.
3. Check the Automatically Execute check box.
4. Click Upload. Follow the on-screen prompts.
   - The upload progress is shown at the bottom of the page.
   - The safety checks and update may take several minutes.
5. When the Update Progress is shown as complete and rebooting, refresh the page.

   ![Update Progress]

   Update Complete, Rebooting...

   Update requested reboot. Rebooting system...

7. Review the software version shown on the Home page. Confirm the Version field shows v7.0.3.
   - Log: Click Support > Update. Click View Log for details.
   - Reload: If you have trouble loading any of the pages, clear your browser cache, close and re-open your browser, and log in again.
8. **Root Partition:** Check the root partition on your appliance.

- Click Home.
- Locate the **Disk Usage** section.
- 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.

5. **Add the Appliance to Central Management**

We recommend that you set up all appliances so they are managed by a Central Manager, which is your primary SMC. Please refer to **Managed and Stand-Alone Requirements in Central Management** to determine if you need to add an appliance to Central Management.

- **SMC Management:** When your appliances are managed by your Stealthwatch Management Console (SMC), you can use Central Management to edit appliance configurations, update software, reboot, shut down, and more.
- **Stand-Alone Appliances:** If an appliance is not managed by the SMC, it is described as a stand-alone appliance. Refer to **Managed and Stand-Alone**
**Requirements in Central Management** (Central Management Requirements column) for the list of appliances that can operate as stand-alone.

With the exception of the Endpoint Concentrator, we recommend that you set up all appliances so they are managed by your primary SMC.

**Best Practices**

To configure your system successfully, make sure you follow the instructions in the *Stealthwatch Installation and Configuration Guide*.

We recommend the following:

- **One at a Time:** Configure one appliance at a time. Confirm the appliance is Up before you start configuring the next appliance in your cluster.
- **Order:** If you are adding more than one appliance to Central Management, follow the configuration order.
- **Managed:** Set up your appliances so they are managed by your primary SMC when possible.
- **Multiple Central Managers:** You can configure more than one Central Manager in your system. However, each appliance can be managed by only one primary SMC/Central Manager.
- **Access:** You need administrator privileges to access Central Management.
- **Custom Certificates:** If your appliance has custom certificates, make sure you save the identity certificate and certificate chain (root and intermediate) individually to its own Trust Store and the SMC Trust Store before you add the appliance to Central Management. Refer to the Trust Store procedure in Stealthwatch Online Help. For details, refer to **Custom Certificates** in the Before you Begin section.
Managed and Stand-Alone Requirements in Central Management

Review the following table to determine if you need to add an appliance to Central Management.

If you are adding more than one appliance to Central Management, make sure you configure your appliances in order, and note the details for each appliance. Refer to the Stealthwatch Installation and Configuration Guide for details.

<table>
<thead>
<tr>
<th>Order</th>
<th>Appliance</th>
<th>Central Management</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Primary SMC</td>
<td>Managed</td>
<td>Your primary SMC is your Central Manager. Make sure the SMC is shown as Up before you start configuring the next appliance in the system.</td>
</tr>
<tr>
<td>2.</td>
<td>UDP Directors (also known as FlowReplicators)</td>
<td>Managed or Stand-Alone</td>
<td>Make sure the Flow Collector 5000 series database is shown as Up before you start the engine configuration.</td>
</tr>
<tr>
<td>3.</td>
<td>Flow Collector 5000 Series Database</td>
<td>Managed</td>
<td>Make sure the Flow Collector 5000 series database is shown as Up before you start the engine configuration.</td>
</tr>
<tr>
<td>4.</td>
<td>Flow Collector 5000 Series Engine</td>
<td>Managed</td>
<td>Make sure the Flow Collector 5000 series database is shown as Up before you start the engine configuration.</td>
</tr>
<tr>
<td>5.</td>
<td>All Other Flow Collectors (NetFlow and sFlow)</td>
<td>Managed</td>
<td>Make sure your Flow Collector is shown as Up before you start the Flow Sensors.</td>
</tr>
<tr>
<td>6.</td>
<td>Flow Sensors</td>
<td>Managed or Stand-Alone</td>
<td>Make sure your Flow Collector is shown as Up before you start the Flow Sensors.</td>
</tr>
</tbody>
</table>
Add the Appliance to Central Management

1. **Open the Appliance Setup Tool:** In your browser address bar, add /*lc-ast after your IP address:

   https://<IPaddress>/lc-ast

2. Use the Appliance Setup Tool to add the appliance to a primary SMC/Central Manager. Refer to the appliance *Installation and Configuration Guide* for details.
3. If you have another stand-alone appliance to update, repeat procedure 15. **Update Stand-Alone orDisconnected Appliances.**
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.)
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)