Cisco Stealthwatch

Update Guide 7.1.3

Table of Contents

Introduction

Overview

Use this guide to update the following Stealthwatch appliances from **v7.0.0** (or a later version of 7.0.x, such as 7.0.2) **to v7.1.3**:

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

For details about v7.1.3, 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). If an appliance is managed by the SMC, it is shown in your Central Management inventory.

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 Begin

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

Software Version

To update the appliance software to version 7.1.3, the appliance must have version **7.0.0** (or a later version of 7.0.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:

- **Update your appliance software versions incrementally:** For example, if you have Stealthwatch v6.9.x, make sure you update each appliance from v6.9.x to v6.10.x, and then v6.10.x to v7.0.x. Each update guide is available on Cisco.com.
- **Patches:** For each software version, make sure you install the latest patches on your appliances before you upgrade. Follow the instructions in this guide.
- **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 v1.2.

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.
- **Certificates:** Some browsers have changed their expiration date requirements for appliance identity certificates. If you cannot access your appliance, log in to the

appliance from a different browser, replace the appliance identity certificate with a custom certificate, or contact Cisco Stealthwatch Support.

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

Licensing

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

- **Check:** Log in to the SMC. Select the **Global Settings** icon > **Central Management**. Review the License Status column.
- **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.

Passwords

We updated the password hashing mechanism in Stealthwatch v6.10.x. As part of the update to Stealthwatch v7.1.3, the SWU will run a safety check to confirm your appliances have compatible password hashing.

- **Before the Update:** If your appliance admin passwords and user passwords have not been changed since v6.9.x, change your passwords before you start the v7.1.3 update using the instructions in this section. If you cannot log in to the appliance, reset your admin password using the Stealthwatch Installation and Configuration Guide.
- **Safety Check:** If your appliances do not pass the safety check during the v7.1.3 update, use the instructions in this section to change your admin passwords and all user passwords for each appliance. If you cannot log in to the appliance, reset your admin password using the Stealthwatch Installation and Configuration Guide.

⚠ If you have not changed your passwords since v6.9, your system is at risk.

Check the Password Policy

1. Log in to the Stealthwatch Management Console. Select the **Global Settings** icon > **Central Management**.
2. Click **Actions** > **Edit Appliance Configuration** > **General**. Under Password Policy, review the **Passwords Expire After** field.
3. Determine if your policy would have triggered users to change passwords after your Stealthwatch Management Console was upgraded from v6.9. Check the password policy on every appliance in Central Management.

Change Passwords on the SMC

If user passwords were not changed since v6.9, you can change all user passwords in User Management. Make sure you change the admin password and the passwords for each user.

1. Log in to the Stealthwatch Management Console as the admin user. Select the **Global Settings** icon > **User Management**.
2. Select a user. Click **Actions** > **Change Password**.
3. Follow the on-screen prompts to change the user password.
4. Repeat steps 2 through 3 for every user in the list.

Change Passwords on All Other Appliances

Use the following instructions to change the admin user password on each Flow Collector, Flow Sensor, UDP Director, and Endpoint Concentrator.

1. Log in to the Appliance Administration interface as the admin.
2. Select **Manage Users** > **Change Password**.
3. Enter the current password and new password.
4. Click **Apply**. Follow the on-screen prompts to change the password.
5. Repeat steps 1 through 4 on each appliance.

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 details.

Disk Space

As part of the update preparation, you will confirm you have enough available disk space on each appliance to install patches and software update files. Refer to **7. Check the Available Disk Space** for instructions.

- **Requirement:** On each managed appliance, you need at least 4 times the size of the individual software update file (SWU) available. On the SMC, you need at least 4 times the size of all appliance SWU files that you upload to Update Manager.
- **Managed Appliances:** For example, if the Flow Collector SWU file is 6 GB, you need at least 24 GB available on the Flow Collector partition (1 SWU file x 6 GB x 4 = 24 GB available).
- **SMC:** For example, if you upload 4 SWU files to the SMC that are each 6 GB, you need at least 96 GB available on the SMC partition (4 SWU files x 6 GB x 4 = 96 GB available).

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. Also, make sure each appliance host name meets the Internet standard requirements for Internet hosts.
- **Check Managed Appliances:** Log in to the SMC. Select the **Global Settings** icon > **Central Management**. Check the Host Name column for each appliance.
- **Check Stand-Alone Appliances:** 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 Managed Appliances:** Log in to the SMC. Select the **Global Settings** icon > **Central Management**. Click the Actions menu for the appliance. Select **Edit Appliance Configuration**. On the Appliance tab, review **Host Naming**.

- **Check Stand-Alone Appliances:** 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.
- **Check Managed Appliances:** Log in to the SMC. Select the **Global Settings** icon > **Central Management**. Click the Actions menu for the appliance. Select **Edit Appliance Configuration**. On the Network Services tab, review **NTP Server**.
- **Check Stand-Alone Appliances:** 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).

- **Configuration:** Before you start the update, make sure your appliances are set to UTC.
- **Virtual Host Server:** Make sure your virtual host server is set to the correct time with respect to UTC.

> ⚠ 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

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.

To update a custom certificate, request an updated certificate from your provider.

- **Update Managed Appliances:** Log in to the SMC. Select the **Global Settings** icon > **Central Management**. Click the Actions menu for the appliance. Select **Edit Appliance Configuration**.

Click the Help icon. Select Stealthwatch Online Help. Review the following help pages for instructions: SSL/TLS Identities and Trust Store.

- **Update Stand-Alone Appliances:** Log in to the Appliance Administration interface. To install the updated certificate from your provider, select **Configuration** > **SSL Certificate**.

  For instructions, 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 Managed Appliances:** Log in to the SMC. Select the **Global Settings** icon > **Central Management**. Click the Actions menu for the appliance. Select **Edit Appliance Configuration**. On the General tab, review **Trust Store**.
- **Check Stand-Alone Appliances:** Log in to the Appliance Administration interface. Select **Configuration** > **Certificate Authority Certificates**.

  For instructions, 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 will need the backup files if there is 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:** 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 Central Management. Doing so will cause the SMC to lose all of the historical data for those Flow Collectors.

- **Flow Collector Update Duration:** We've added process improvements to Stealthwatch Flow Collectors as part of this software update. The update may take up to 2 hours to finish.

  Make sure the Flow Collector update is completed and the appliance status is shown as Up before you update the next appliance in your cluster.

  Flow Collector 5000 Series: Make sure the database update is completed and the appliance status is shown as Up before you start the engine update. Then, make sure the engine update is completed and the appliance status is shown as Up before you update the next appliance in your cluster.

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 Stealthwatch Desktop Client will display a red “x” and the managed appliance icon will be orange () 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 Stealthwatch Desktop Client. When the update is complete, communications are re-established, the icons return to normal appearance, and the alarm disappears.

Alternative Access

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

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

Hardware

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

Virtual Machines

Console (serial connection to console port): Refer to the latest KVM or VMware documentation for your appliance installation.

- For example, for **KVM**, refer to Virtual Manager documentation.
- For **VMware**, refer to the vCenter Server Appliance Management Interface documentation for vSphere.

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.

Enabling SSH in Central Management

Use this section to control the ability to access the appliance using SSH (secure shell). If you cannot log in to an appliance using the virtual or hardware methods, you can enable SSH on the appliance 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.

Open SSH

Use the following instructions to open SSH for a selected appliance.

1. Open **Central Management** > **Appliance Manager**.
2. Click **Actions** menu for the appliance.
3. Select **Edit Appliance Configuration**.
4. Select the **Appliance** tab.

Enable SSH

1. Locate the **SSH** section.
2. Select whether to enable SSH access only or to also enable root access.
    - **Enable SSH:** To allow SSH access on the appliance, check the check box.
    - **Enable Root SSH Access:** To allow root access on the appliance, check the check box.
3. Click **Apply Settings**.
4. Follow the on-screen prompts.

> ⚠ 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.

Enabling SSH in Appliance Admin Interface

Use the following instructions to open SSH for a stand-alone appliance through the Appliance Admin Interface.

1. Log in to the Appliance Admin interface.
2. Click **Configuration** > **Services**.
3. Check the **Enable SSH** check box to allow access to SSH.
4. Check the **Enable Root SSH Access** check box to also allow access to root.
5. Click **Apply**.

> ⚠ 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.

Update Overview

> ⚠ Make sure you follow the software installation order for 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 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
8. Back Up the Update Log
9. Install Patches
10. Install the v7.1.3 Software Update. Use Central Management to update each managed appliance. Make sure you install the v7.1.3 SWU using the update order.
11. Install the Stealthwatch Desktop Client
12. Verify SMC Failover Roles
13. Update Stand-Alone Appliances. Also, 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.

1. Review Your Cluster

Use the following instructions to review your Stealthwatch appliances.

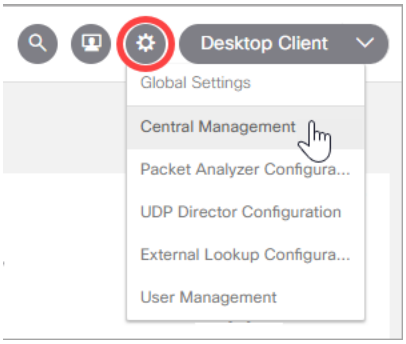
- **Central Management:** Configure all Stealthwatch appliances so they are managed by your Stealthwatch Management Console (SMC). To review all appliances managed by the SMC, review the Central Management > Appliance Manager page. To add an appliance to Central Management, refer to the Stealthwatch Installation and Configuration Guide v7.0 for details.
- **SMC Maximum:** You can update two SMCs for this update.
- **Stand-Alone Appliances:** If you have an Endpoint Concentrator or other appliance that will remain un-managed, you can update the appliance after the 7.1.3 update to managed appliances is completed. Refer to **13. Update Stand-Alone 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 stand-alone appliances to Central Management after the v7.1.3 update is completed.

2. Confirm the Installed Software Version

To verify that the current software version for each appliance is **v7.0.0** (or a later version of 7.0.x, such as 7.0.2) complete the following steps:

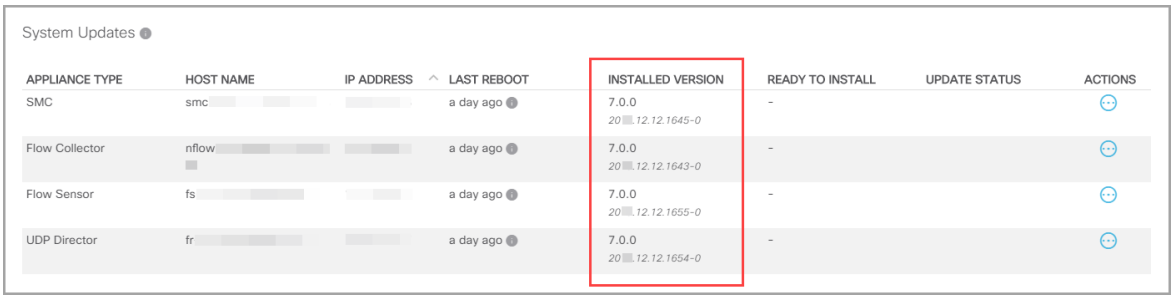
1. Log in to your SMC.
   (In your browser address field, type https:// and the appliance IP address. Press Enter.)
2. Click the **Global Settings** icon.
3. Select **Central Management**.



4. Select the **Update Manager** tab, and locate the **System Updates** section.
5. Review the **Installed Version** column. Confirm each appliance has **v7.0.0** (or a later version of 7.0.x) installed.

   Same Version: Make sure all appliances are using the same software version. For example, if your SMC has v7.0.2 installed, the other appliances in your cluster need to have 7.0.2 installed.

   6.10.x or earlier: If the software version is 6.10.x or earlier, update the appliance to 7.0.x) before you start this update. See the Stealthwatch System Update Guide.

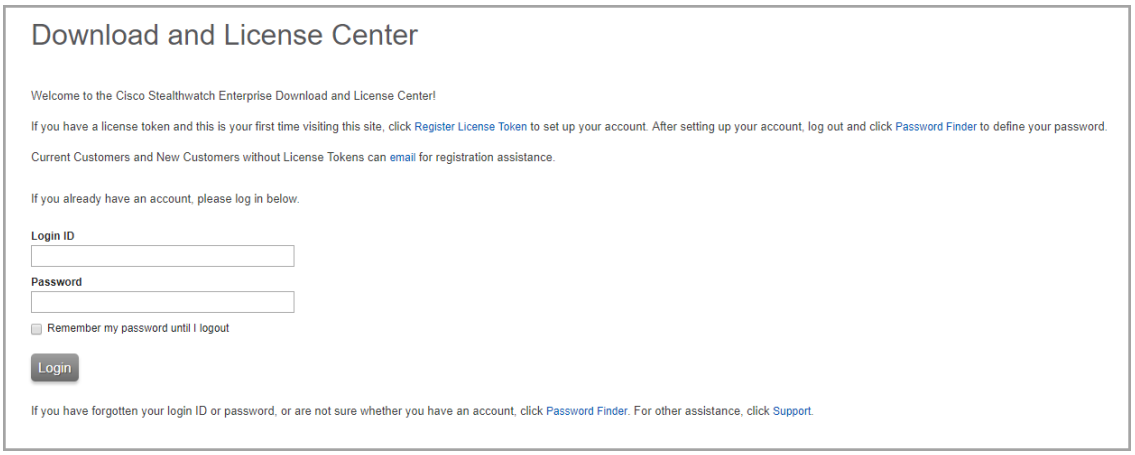


Make sure every appliance has the correct software version installed. This step is critical for a successful update.

3. Download the Patches and Update Files

Use the following instructions to download patches and the v7.1.3 SWUs listed on your account.

1. Go to https://stealthwatch.flexnetoperations.com.



2. Log in to the Cisco Stealthwatch Enterprise Download and License Center.
3. Select **Downloads** > **Patch Stealthwatch**.
4. Download all patches for each appliance.

   You may see appliance-specific rollup patches and/or common patches to apply to all appliances. Make sure you download all of them.

5. Select **Downloads** > **Upgrade Stealthwatch**.
6. On the **Current Versions** tab, click the appliance name. Click the software release link to download it (or select FTP Download).

   - **SWUs:** Each appliance has one unified update file for both the virtual (VE) and physical appliance.
   - Download the 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.

SWU Files

Appliance	Update File Name
UDP Director (also known as Flow Replicator) UDP Director VE (also known as Flow Replicator VE)	update-udpd-7.1.3.2020.06.16.1331-01.swu
Flow Collector 5000 series Database	update-fcdb-7.1.3.2020.06.16.1333-01.swu
Flow Collector for NetFlow (This is needed for the Flow Collector 5000 series engine) Flow Collector for NetFlow VE	update-fcnf-7.1.3.2020.06.16.1334-01.swu
Flow Collector for sFlow Flow Collector for sFlow VE	update-fcsf-7.1.3.2020.06.16.1333-01.swu
Endpoint Concentrator	update-ec-7.1.3.2020.06.16.1331-01.swu
SMC and SMC VE	update-smc-7.1.3.2020.06.16.1337-01.swu
Flow Sensor Appliance Flow Sensor VE	update-fsuf-7.1.3.2020.06.16.1331-01.swu

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.

Create a Backup Configuration File

Use the following instructions to select an appliance from the Appliance Manager and create a backup file of the configuration settings.

1. Open **Central Management** > **Appliance Manager**.
2. Click the **Actions** menu for the SMC.

    - **All Managed Appliances:** To back up the configuration of all appliances managed by the Central Manager, select your primary SMC.
    - **Individual Managed Appliance:** To back up the configuration of an individual appliance in Central Management, select the Actions menu for the appliance. For example, if you only need to back up your Flow Sensor, select the Flow Sensor Actions menu.

3. Select **Support**.
4. Select the **Configuration Files** tab.
5. Click the **Backup Actions** drop-down.
6. Select **Create Backup**.

> ⚠ If you are backing up an SMC or Flow Collector, you also have to back up the databases. You need both backups to restore these appliances completely. Refer to **6. Back Up the Flow Collector and SMC Databases** for instructions.

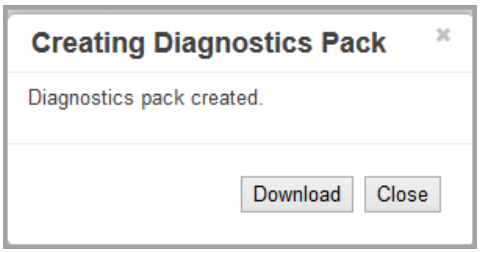
5. Create a Diagnostics Pack

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. Log in to the Appliance Admin interface.
2. Click **Support** > **Diagnostics Pack**.
3. Click **Create Diagnostics Pack**.

4. Click **Download** and save the diagnostics pack (GPG) file to your preferred location. This process may take a few minutes.



5. 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 Stealthwatch Management Console (SMC), back up the Flow Collector database and SMC database. For assistance, please contact Cisco Stealthwatch Support.

> 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 for an SMC**
2. **Trim the Flow Collector Database**
3. **Back Up the Databases**
4. **Delete the Database Snapshots**
5. **Re-enable SNMP Polling in the SMC**

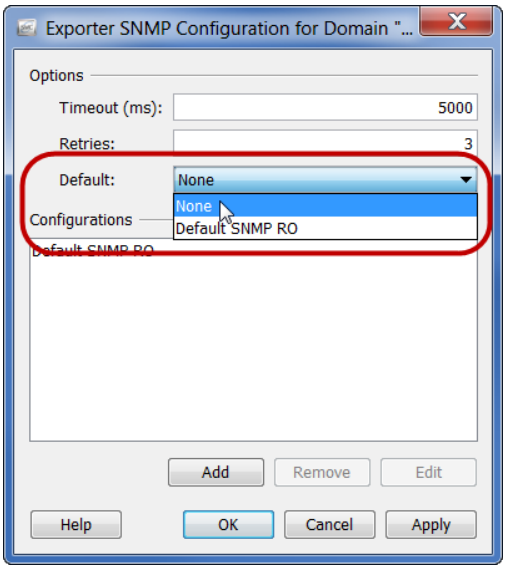
> Without a backup, you will not be able to recover your files if a problem occurs during the update process. Make sure you follow the instructions and complete all procedures for the database backup. For assistance, please contact Cisco Stealthwatch Support.

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 Stealthwatch 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 through 6 for each domain on your system.

2. Trim the Flow Collector Database

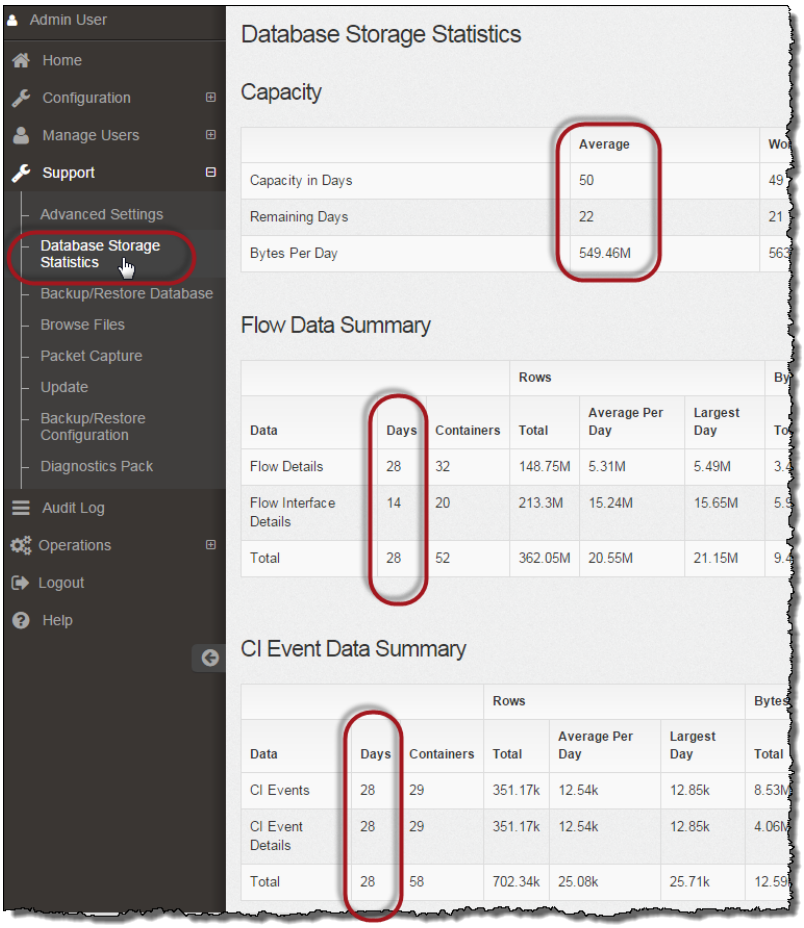
The Flow Collector database backup may take multiple days to finish and will slow your network speed if the database is large. Before you back up your databases, we recommend trimming the Flow Collector database. This will free the available disk space for storing flows and reduce the amount of time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

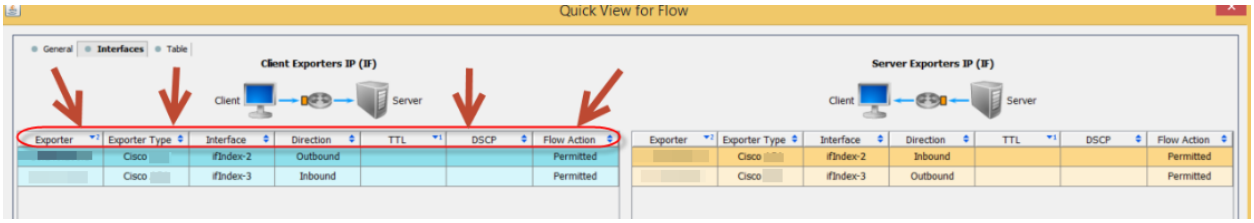
Use the following instructions to check your database storage.

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 (or Security 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.



Backing up this data takes time. If you don't need all of it, shorten the storage limit (for example: 7 days). Any data older than the limit will be lost.

Use the following instructions to purge the database of the interface statistics data older than the limit you set, 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.
3. Right-click the Flow Collector. Select **Configuration** > **Properties**.
4. In the Flow Collector Properties dialog box, click **Advanced**.
5. Select the **Store flow interface data**.
6. Shorten the storage limit.

   For example, if you set the limit to **Up to 7 days**, anything older than 7 days will be lost.
7. Click **OK**.
8. Wait 5 minutes to proceed to the next steps.

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.

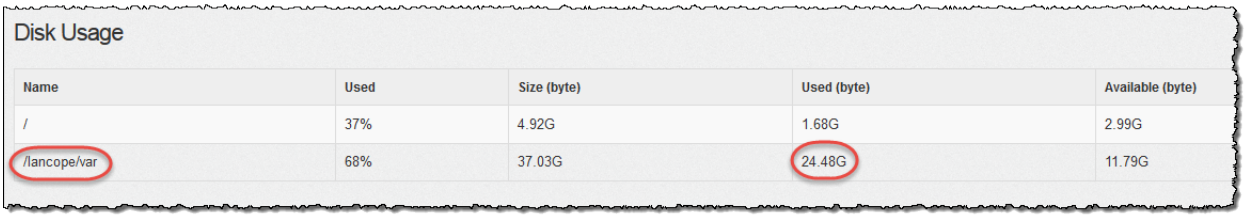
3. Back Up the Databases

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

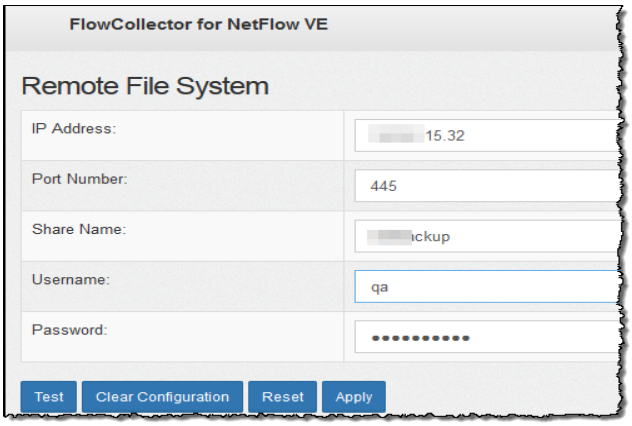
- **Space:** Make sure the remote file system has enough space to store the database backup.
- **Time:** After you back up the database once, subsequent backups will be quicker because the process backs up only what has changed since the last backup. This process backs up approximately 0.5 GB to 2 GB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

1. Return to the Appliance Admin interface (but do not close the 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.

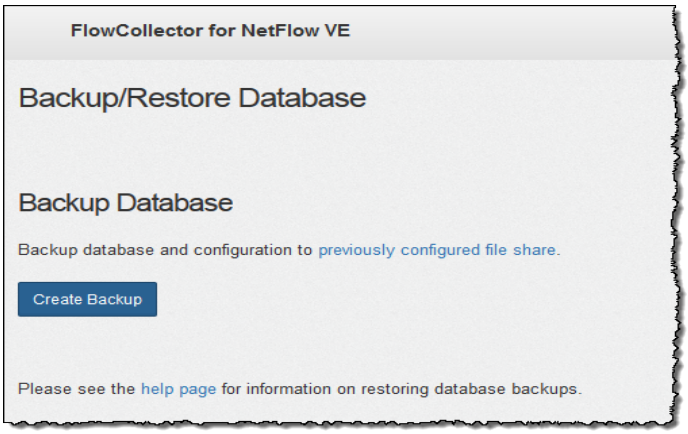
6. Click **Test** to verify that the Stealthwatch appliance and the remote file system can communicate with each other.

   You should see the following message at the bottom of the Remote File System

page when the test is complete.

File sharing appears to be properly configured.

7. Click **Support** > **Backup/Restore Database**. The Backup Database page opens as shown in the following example.



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**.

9. Click **Close** to close the progress window.

4. Delete the Database Snapshots

After you have saved the backup files, use the following instructions to delete the snapshots on the SMC and Flow Collector databases.

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

1. Log in to the SMC or Flow Collector console as **admin**.
2. **Check for Snapshots:** Type:

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

3. **Delete Snapshots (if they exist):** Type:

   ```
   /opt/vertica/bin/vsql -U dbadmin -w lan1cope -c "select remove_database_snapshot('StealthWatchSnap1');"
   ```

4. Repeat steps 1 through 3 to delete all saved SMC and 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 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 4 in Disabling SNMP Polling). SNMP polling for this domain is now re-enabled.
4. Click **OK**.
5. Repeat steps 2 through 4 in this procedure for each domain on your system.
6. Close the Desktop Client.

7. Check the Available Disk Space

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

> ⚠ Make sure you have enough available space on the SMC for all appliance SWU files that you upload to Update Manager. Also, confirm you have enough available space on each individual appliance.

- **SMC:** When the SWU is uploaded to the Update Manager in Central Management, it will use additional space on the SMC during the update. The file remains on the SMC (Central Management) until it is replaced by another file of the same type. Make sure you have enough available space on the SMC for all appliance SWU files that you upload to Update Manager.

  For example, if you update a Flow Collector through the Update Manager in Central Management, the file remains in the SMC file system until you upload a new Flow Collector SWU file.

- **Managed Appliances:** If you update an appliance through the Update Manager in Central Management, the SWU will be removed from the appliance file system after the update is completed.

  For example, if you update a Flow Collector through the Update Manager in Central Management, the file will be removed from the Flow Collector file system after the update is completed.

Check the Available Disk Space

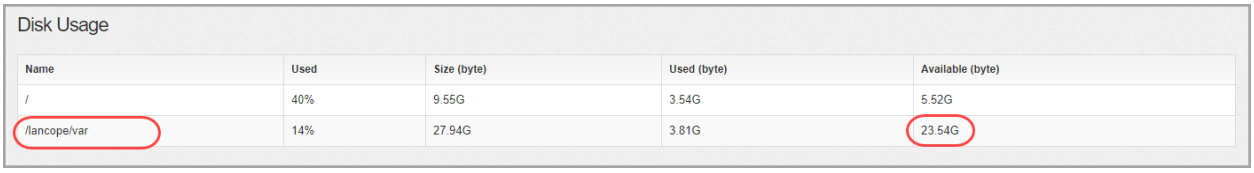
Use these instructions to confirm you have enough available disk space to install patches and software update files on the SMC and each managed appliance.

1. Log in to the Appliance Admin interface.
2. Click **Home**.
3. Locate the **Disk Usage** section.
4. Review the **Available (byte)** column and confirm that you have the required disk space available on the **/lancope/var/** partition.

   - **Requirement:** On each managed appliance, you need at least 4 times the

size of the individual software update file (SWU) available. On the SMC, you need at least 4 times the size of all appliance SWU files that you upload to Update Manager.

- **Managed Appliances:** For example, if the Flow Collector SWU file is 6 GB, you need at least 24 GB available on the Flow Collector partition (1 SWU file x 6 GB x 4 = 24 GB available).
- **SMC:** For example, if you upload 4 SWU files to the SMC that are each 6 GB, you need at least 96 GB available on the SMC partition (4 SWU files x 6 GB x 4 = 96 GB available).



5. If you need to expand the appliance disk space, see the Data Storage section of the Stealthwatch Installation and Configuration Guide v7.0 for your appliance.

8. Back Up the Update Log

Use these instructions to back up the update log in each appliance. Make sure you create a backup of the update log on every appliance in your Stealthwatch cluster.

1. SSH in to the appliance.
2. Log in as root.
3. Type the following:

```
cp /lancope/var/admin/upgrade/upgradeOutput.log /lancope/var/
admin/upgrade/upgradeOutputHistory.log
```

4. Press Enter.
5. Exit the appliance.
6. Repeat this procedure on every appliance in your Stealthwatch cluster.

> ⚠ Confirm you've completed procedures 1 through 8 on every managed appliance in your Stealthwatch cluster before you start the next procedure **9. Install Patches**.

9. Install Patches

Before you start the software update, make sure you install the latest patches on your appliances. To download patches, refer to **3. Download the Patches and Update Files** for details.

You can upload a patch file for a specific appliance or upload a common patch, which will apply to all appliances in Central Management. Refer to the Patch Readme Notes for details.

> Make sure the appliance status is shown as Up before you install any patches.

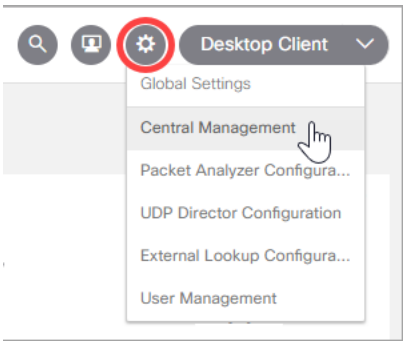
Best Practices

- **Readme:** Refer to the Patch Readme Notes for details.
- **Order:** Make sure you apply patches on 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 1 hour and less than 7 days before you install the patch.
- **Confirm:** Confirm the update is installed and that each appliance status is shown as Up before you start the next appliance update.

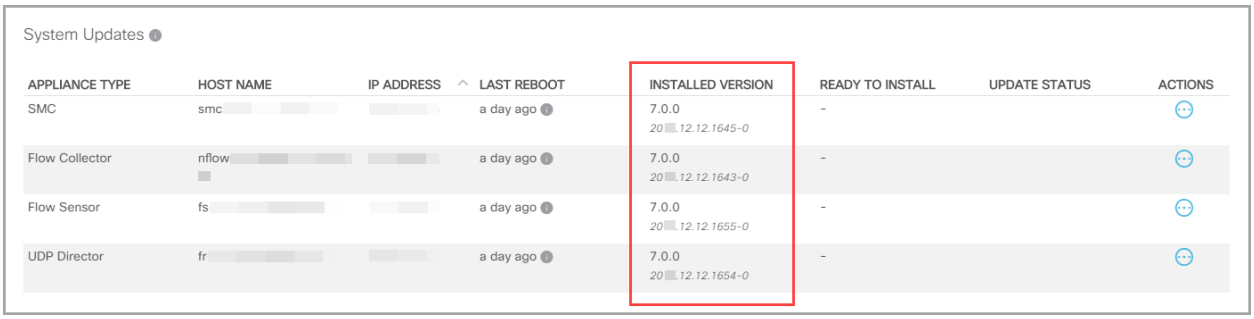
1. Upload Patches

Use these instructions to upload patches to the Update Manager in Central Management.

1. Log in to your SMC.
   (In your browser address field, type https:// and the appliance IP address. Press Enter.)
2. Click the **Global Settings** icon.
3. Select **Central Management**.



4. Select the **Update Manager** tab, and locate the **System Updates** section.
5. Review the **Installed Version** column. Confirm each appliance has **v7.0.0** (or the latest version of 7.0.x) installed.



6. Click **Upload**.
7. Follow the on-screen prompts to select a patch SWU file. Upload one file at a time.

    - **Patches:** Upload a patch file for a specific appliance or upload a common patch, which will apply to all appliances in Central Management. Refer to the Patch Readme Notes for details.

    - **Disk Space:** For details, refer to Check the Available Disk Space.

2. Install Patches

Use the following instructions to apply a patch using Central Management.

1. In the **Update Manager** > **System Updates** section, check the following columns for the appliance to confirm it is ready to update:
   - **Ready to Install:** Confirm the patch file is posted.
   - **Last Reboot (SMCs and Flow Collectors):** Make sure the last reboot as was more than 1 hour and less than 7 days.
     - If it is less than 1 hour, wait to proceed.
     - If it is more than 7 days, click **Actions** menu > **Reboot Appliance** to restart the appliance. Wait for at least 1 hour to confirm that all processes and safety checks are ready.

> ⚠ Do not reboot the appliance while configuration changes are pending or if the configuration channel is down. To confirm the appliance status is Up, review the Central Management > Appliance Manager page.

2. Click the **Actions** menu for the appliance.
3. Select **Install Update**.
4. Follow the on-screen prompts to confirm the update.
   - **Update Status:** The update status column will change from Waiting to Install… to Installing. The screen refreshes every 1 minute.
   - **Reboot:** The appliance reboots automatically for software updates. Refer to the Patch Readme Notes for details.

3. Confirm the Patch Installation

Patches do not change the information shown in the Installed Version column. Use the following instructions to check the update log.

1. Click the **Actions** menu for the appliance.
2. Select **View Update Log**.
3. Confirm the patch is listed as successful or installed.

   Unsuccessful: If the patch was unsuccessful, correct any errors and try again. For

more information, refer to Troubleshooting Errors.

4. Review the appliances on the Central Management > Appliance Manager page.

   - **Appliance Status:** 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**.

5. Repeat all steps in this section to install the latest patches on each appliance in your cluster.

10. Install the v7.1.3 Software Update

You will continue using the Update Manager page for the software update.

> ⚠ Make sure your SMC and Flow Collectors have been running for more than 1 hour and less than 7 days before you start the software update.

Use the Update Order

Update your appliances in the following order:

Order	Appliance	Notes
1.	UDP Directors (also known as Flow Replicators)	If you have a High Availability cluster, update the secondary UDP Director first. Confirm the update is completed and the secondary UDP Director appliance status is shown as Up before you update the primary UDP Director.
2.	Flow Collector 5000 Series Database	Make sure the Flow Collector has been running for more than 1 hour and less than 7 days before you start the update. Make sure the database update is completed and the appliance status is shown as Up before you start the engine update. The update may take up to 2 hours to finish.
3.	Flow Collector 5000 Series Engine	Make sure the Flow Collector 5000 series database completes the update and the appliance status is shown as Up before you start the engine update. Make sure the engine update is completed and the appliance status is

		shown as Up before you update the next appliance in your cluster. The update may take up to 2 hours to finish.
4.	All Other Flow Collectors (NetFlow and sFlow)	Make sure the Flow Collector has been running for more than 1 hour and less than 7 days before you start the update. Make sure the Flow Collector update is completed and the appliance status is shown as Up before you update the next appliance in your cluster. The update may take up to 2 hours to finish.
5.	Secondary SMC (if used)	Make sure the SMC has been running for more than 1 hour and less than 7 days before you start the update. If your system uses a secondary SMC, confirm the secondary SMC update is completed and confirm the secondary SMC appliance status is shown as Up before you start the primary SMC update. After the update completes, both SMCs may restart in the secondary role. If this occurs, see **12. Verify SMC Failover Roles** for details. Do not change the failover roles until both SMCs are updated.
6.	Primary SMC	Make sure the SMC has been running for more than 1 hour and less than 7 days before you start the update. If your system uses a secondary SMC, confirm the secondary SMC update is

		completed and confirm the secondary SMC appliance status is Up before you start the primary SMC update. After the update completes, both SMCs may restart in the secondary role. If this occurs, see **12. Verify SMC Failover Roles** for details. Do not change the failover roles until both SMCs are updated.
7.	Flow Sensors	
8.	Stand-Alone 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 1 hour and less than 7 days before you start the 7.1.x software update.
- **Flow Collectors:** We've added process improvements to Stealthwatch Flow Collectors as part of this software update. The update may take up to 2 hours to finish. Review the details for your Flow Collector in the appliance update order before you start.
- **Confirm:** Confirm the update is installed and that each appliance status is shown as Up 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.

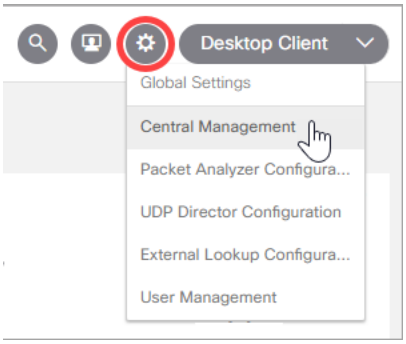
For example, if you have several Flow Sensors in your cluster, you can update all Flow Sensors at the same time. However, make sure you have completed updating all the Flow Collectors in your cluster first.

Install the Software Update on Managed Appliances

Use these instructions to install the software update on appliances in Central Management.

1. Upload the SWUs

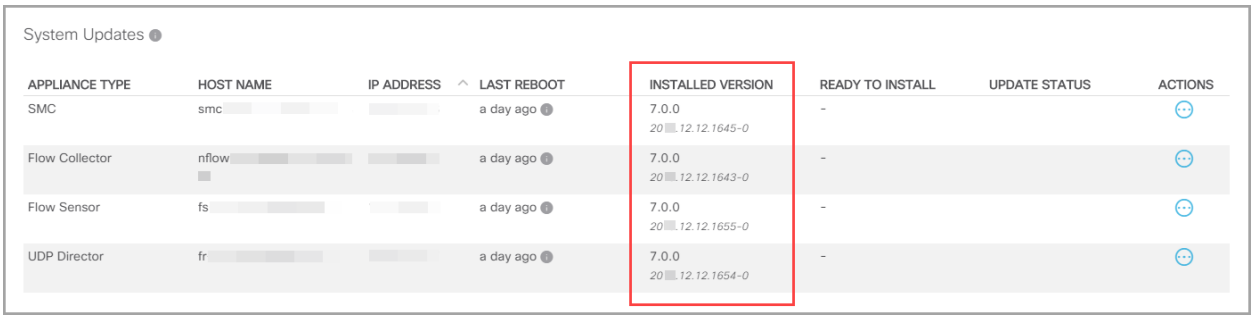
1. Log into your SMC.
   (In your browser address field, type https:// and the appliance IP address. Press Enter.)
2. Click the **Global Settings** icon.
3. Select **Central Management**.



4. Select the **Update Manager** tab, and locate the **System Updates** section.

> ⚠ Make sure you update the appliances in order and review the details before you start. Confirm the update is installed and that each appliance is shown as Up before you start the next appliance update.

5. Review the **Installed Version** column. Confirm each appliance has **v7.0.0** (or the latest version of 7.0.x) installed.



6. Click **Upload**.
7. Follow the on-screen prompts to select a SWU file. Upload one file at a time.

    - **Updates:** Upload a SWU file for each appliance in Central Management.
    - **Disk Space:** For details, refer to Check the Available Disk Space.

2. Install the SWU

Use the following instructions to update the software using Central Management. Make sure you update the appliances in order.

1. In the **Update Manager** > **System Updates** section, check the following columns for the appliance to confirm it is ready to update:

    - **Ready to Install:** Confirm the 7.1.3 SWU file is posted.
    - **Last Reboot (SMCs and Flow Collectors):** Make sure the last reboot was more than 1 hour and less than 7 days.
        - If it is less than 1 hour, wait to proceed.
        - If it is more than 7 days, click **Actions** menu > **Reboot Appliance** to restart the appliance. Wait for at least 1 hour to confirm that all processes and safety checks are ready.

> ⚠ Do not reboot the appliance while configuration changes are pending or if the configuration channel is down. To confirm the appliance status is Up, review the Central Management > Appliance Manager page.

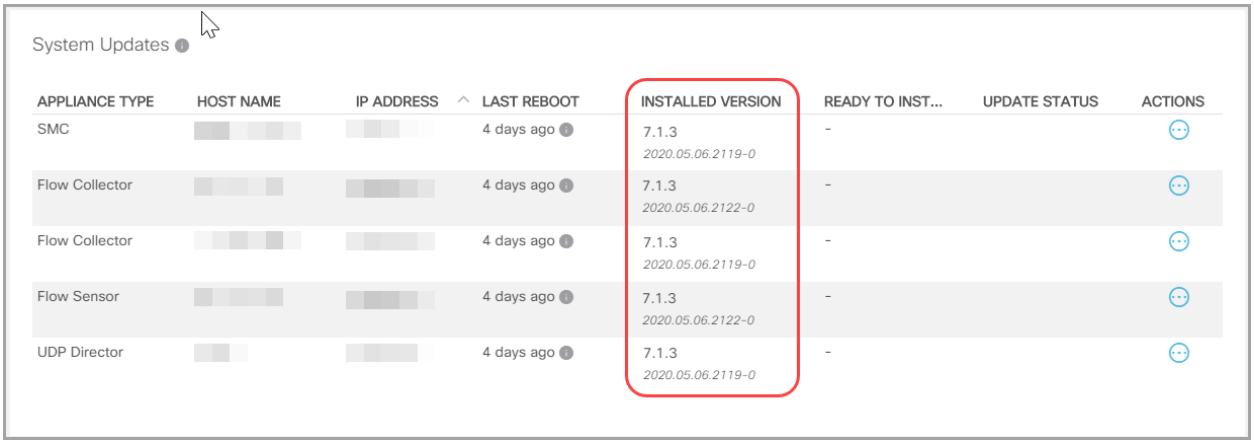
2. Click the **Actions** menu for the appliance.
3. Select **Install Update**.
4. Follow the on-screen prompts to confirm the update.

- **Update Status:** The update status column will change from Waiting to Install… to Installing. The screen refreshes every 1 minute.
- **Reboot:** The appliance reboots automatically for software updates.

> ⚠ The appliance reboots automatically. Do not force the appliance to reboot while configuration changes are pending. If you are updating a Flow Collector database, the update may take up to 2 hours.

3. Confirm the Software Update

1. Check the **Installed Version** column to confirm it shows the **7.1.3** software update.



- **Installation Successful:** If **7.1.3** is shown as the installed version, go to the next step to confirm the appliance status.
- **Install Failed:** If the SWU installation failed, click the appliance **Actions** menu > **View Update Log**. Review the log for errors.
- **Password Error:** Review the log for PASSHASH_ERROR. If the safety check found incompatible password hashing, refer to **Passwords** to reset your passwords.
- **Troubleshooting Errors:** You may find some of the following errors in the log or on the UI:

Error Description or Category	Details
Install Update button is unavailable	If you cannot click the **Install Update** button because it is grayed out, confirm the appliance SWU file is shown in the Ready to Install column. Also, check the **Last Reboot** column to confirm the last reboot on your SMCs and Flow Collectors was more than 1 hour and less than 7 days. • If it is less than 1 hour, wait to proceed. • If it is more than 7 days, go to the Appliance Inventory. Click **Actions** menu > **Reboot Appliance** to restart the appliance. Wait for at least 1 hour to confirm that all processes and safety checks are ready.
Loss of network connectivity between the SMC and managed appliances	Restore the network connectivity and confirm each appliance is shown as **Up** on the Appliance Inventory. If the appliance status is **Config Channel Down**, refer to the Troubleshooting section of the Stealthwatch Installation and Configuration Guide for instructions. Retry the patch or software update file installation after you confirm network connectivity is restored.
`No space left on device` (Disk Space)	Check the disk space on each appliance to confirm you have enough available space to install patches and software update files. On each managed appliance, you need at least 4 times the size of the individual software update file (SWU) available. On the SMC, you need at least 4 times the size of all appliance SWU files that you upload to Update Manager. • **Managed Appliances:** For example, if the Flow Collector SWU file is 6 GB, you need at least 24 GB available on the Flow Collector partition (1 SWU file x 6 GB x 4 = 24 GB

Error Description or Category	Details
	available). • **SMC:** For example, if you upload 4 SWU files to the SMC that are each 6 GB, you need at least 96 GB available on the SMC partition (4 SWU files x 6 GB x 4 = 96 GB available). • **Additional Information:** Refer to **7. Check the Available Disk Space** for instructions.
`Unexpected exit status!`	If you encounter this error, it may be the following: • a service failed to stop cleanly during the installation preparation • the update was started before meeting the reboot requirements Confirm each appliance is shown as **Up** on the Appliance Inventory. If the appliance status is **Config Channel Down**, refer to the Troubleshooting section of the Stealthwatch Installation and Configuration Guide for instructions. Also, check the **Last Reboot** column to confirm the last reboot on your SMCs and Flow Collectors was more than 1 hour and less than 7 days. • If it is less than 1 hour, wait to proceed. • If it is more than 7 days, go to the Appliance Inventory. Click **Actions** menu > **Reboot Appliance** to restart the appliance. Wait for at least 1 hour to confirm that all processes and safety checks are ready.
`Upload Failed`	Make sure you upload one file at a time. We do not support uploading multiple SWU files at the same time. Confirm each upload is completed and shown in

Error Description or Category	Details
	the **Ready to Install** column before you start uploading another SWU file. Refer to **10. Install the v7.1.3 Software Update** for more information.

2. Select the **Appliance Manager** tab. Locate the appliance in the inventory.
    - **Up:** Confirm the appliance status is shown as **Up**.
    - **SMC:** If you have a primary SMC and secondary SMC, confirm the Appliance Status for each SMC is shown as **Up**.
    - **Flow Collector Database:** We've added process improvements to the Flow Collector database as part of this software update. Make sure the database completes the update and the appliance status is shown as **Up** before you start the engine update. This may take up to 2 hours.
3. Repeat all steps in this section, **Install the Software Update on Managed Appliances**, for the next appliance. Make sure you update the appliances in order.
4. If you've updated every appliance in Central Management, go to **11. Install the Stealthwatch Desktop Client**.

11. Install the 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.

   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.

   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.

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.

- 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.

12. Verify SMC Failover Roles

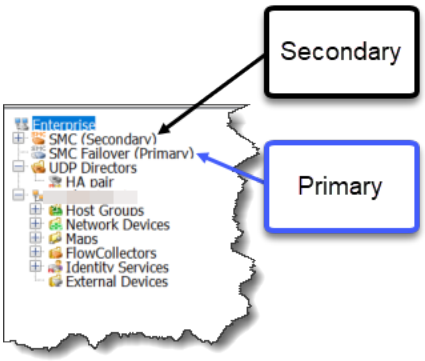
If you do not use the SMC failover configuration, you can skip this procedure.

> ⚠ Do not change the failover roles until both SMCs are updated.

> ⚠ Do not add or remove appliances from Central Management until you have 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 Stealthwatch Desktop Client Help.

> ℹ For instructions, refer to the Stealthwatch Desktop Client Help.

5. Log in to the **secondary SMC** (Stealthwatch 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.
   - Click the **Global Settings** icon. Select 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.

13. Update Stand-Alone Appliances

Use the following instructions to update appliances to v7.1.3 (or a later version of 7.1.x) that have the following scenarios:

- if the appliance is an **Endpoint Concentrator**
- if you have stand-alone appliances that were not updated with the rest of your cluster because they are not currently 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 stand-alone appliances, you are finished with the Stealthwatch update.

1. Download the Patches and Update Files

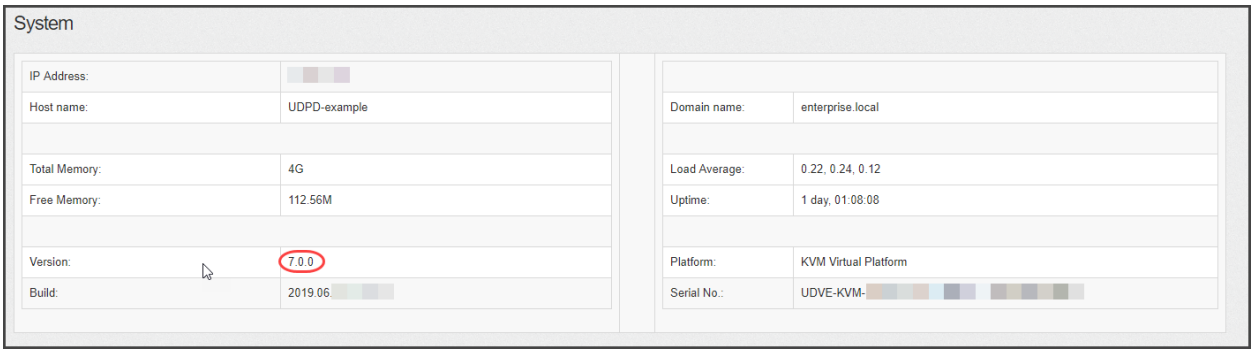
Use the Download the Patches and Update Files procedure to download patches and update files.

2. Check the Software Version

Use the following instructions to confirm the software version on your stand-alone appliance.

1. Log in to the Appliance Admin interface (https://[IP address]).
2. Review the software version shown on the Home page. Confirm the appliance has **v7.0.0** (or a later version of 7.0.x) installed.

   6.10.x or earlier: If the software version is 6.10.x or earlier, update the appliance to 7.0.0 (or the latest version of 7.0.x) before you start this update using the Stealthwatch Update Guide.

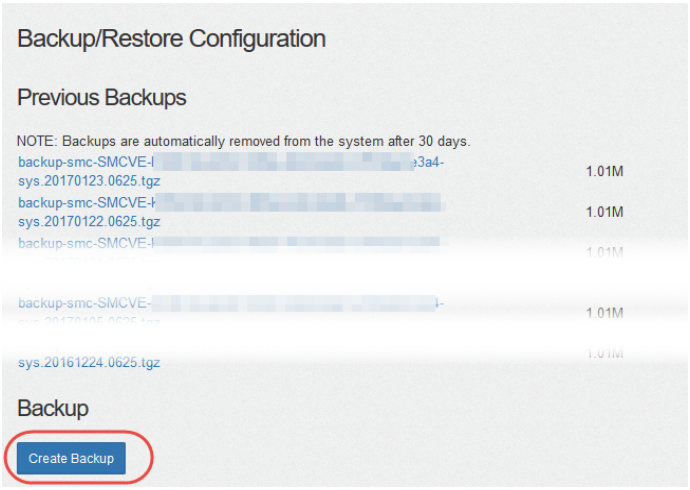


3. Back Up the Appliance Configuration

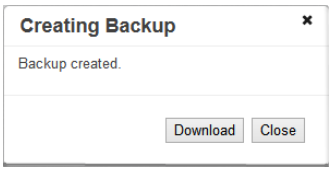
Complete these steps to back up the configuration of a stand-alone appliance. These steps are important to help minimize data loss.

> ⚠ 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.

> ⚠ If you are backing up an SMC or Flow Collector, you also have to back up the databases. You need both backups to restore these appliances completely. Refer to **5. Back Up the Flow Collector and SMC Databases** for instructions.

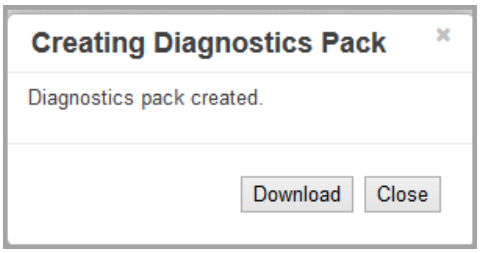
4. Create a Diagnostics Pack

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. Log in to the Appliance Admin interface.
2. Click **Support** > **Diagnostics Pack**.
3. Click **Create Diagnostics Pack**.

4. Click **Download** and save the diagnostics pack (GPG) file to your preferred location. This process may take a few minutes.



5. 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.

5. 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 for an SMC**
2. **Trim the Flow Collector Database**
3. **Back Up the Databases**
4. **Delete the Database Snapshots**
5. **Re-enable SNMP Polling in the SMC**

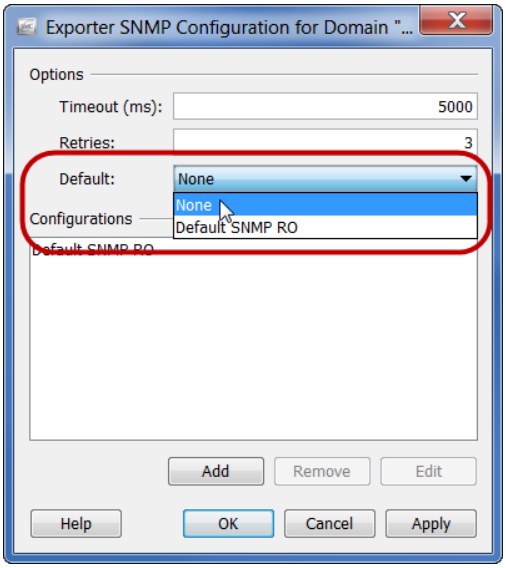
Without a backup, you will not be able to recover your files if a problem occurs during the update process. Make sure you follow the instructions and complete all procedures for the database backup. For assistance, please contact Cisco Stealthwatch Support.

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 Stealthwatch 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 through 6 for each domain on your system.

2. Trim the Flow Collector Database

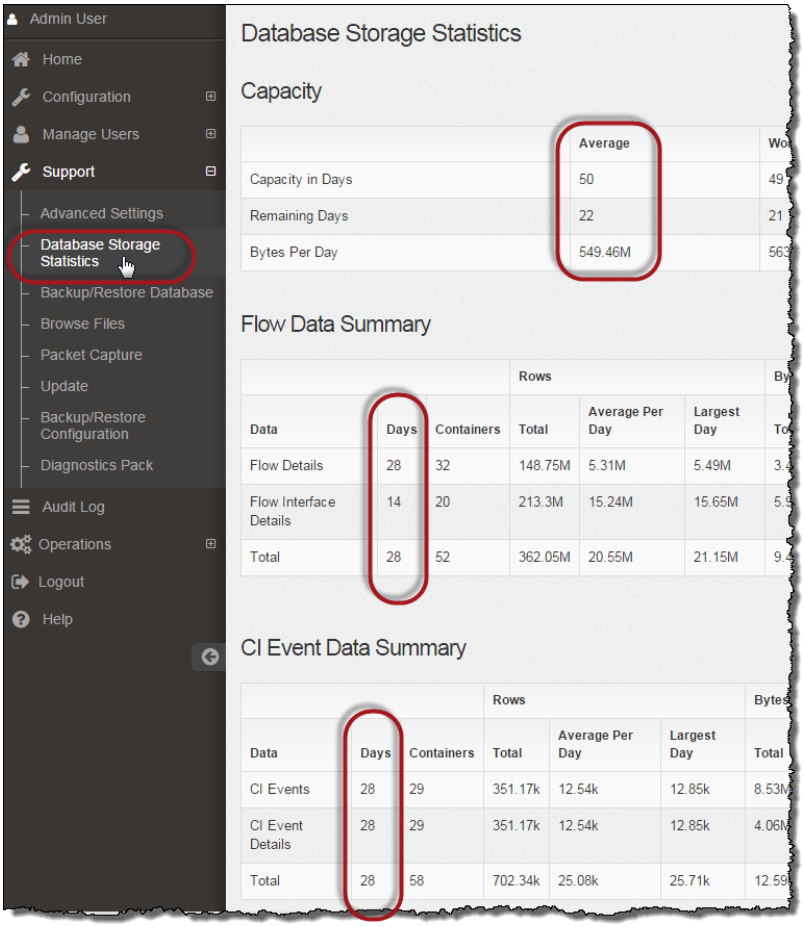
The Flow Collector database backup may take multiple days to finish and will slow your network speed if the database is large. Before you back up your databases, we recommend trimming the Flow Collector database. This will free the available disk space for storing flows and reduce the amount of time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

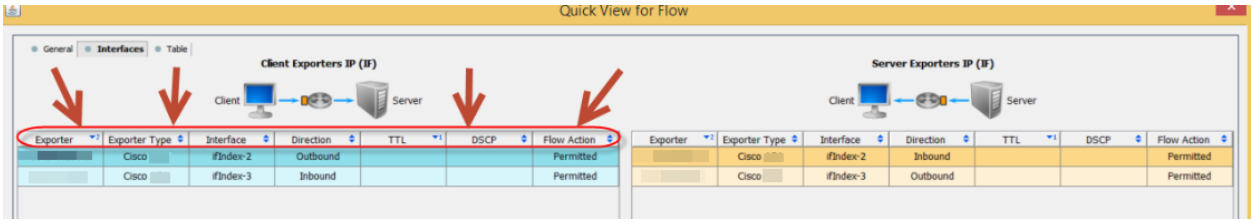
Use the following instructions to check your database storage.

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 (or Security 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.



Backing up this data takes time. If you don't need all of it, shorten the storage limit (for example: 7 days). Any data older than the limit will be lost.

Use the following instructions to purge the database of the interface statistics data older than the limit you set, 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.
3. Right-click the Flow Collector. Select **Configuration** > **Properties**.
4. In the Flow Collector Properties dialog box, click **Advanced**.
5. Select the **Store flow interface data**.
6. Shorten the storage limit.

   For example, if you set the limit to **Up to 7 days**, anything older than 7 days will be lost.
7. Click **OK**.
8. Wait 5 minutes to proceed to the next steps.

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:

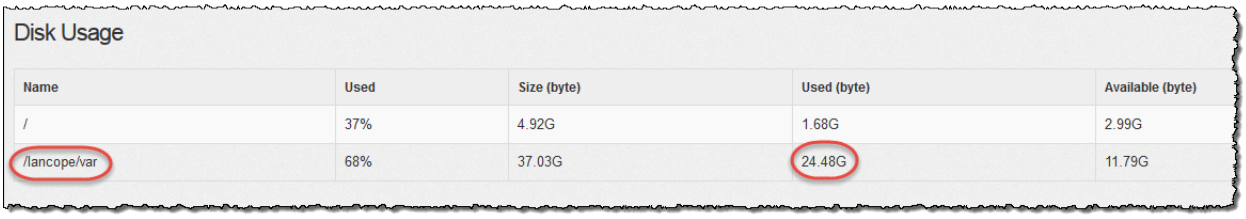
- The database is trimmed down to the number of days you enter.
- The database starts rolling the older data out based on the oldest day but without trying to save as much as possible.

3. Back Up the Databases

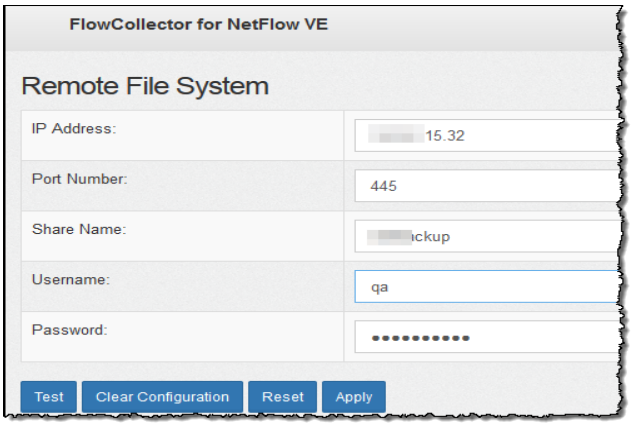
To back up a Flow Collector database or SMC database to a remote file system, complete the following steps:

- **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 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.

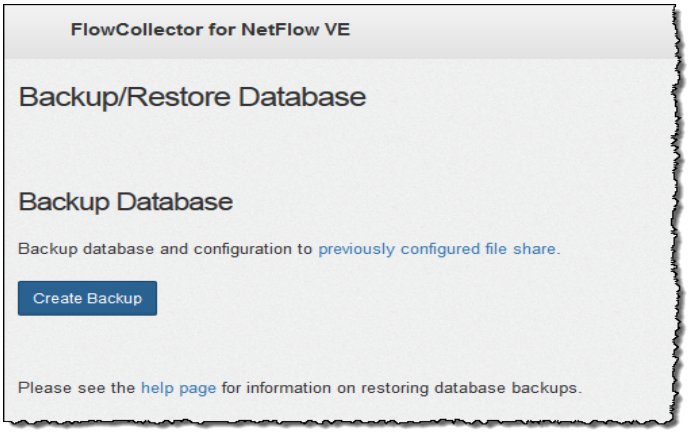
   If the Apply button is not enabled after you enter the password, click once in a blank area on the Remote File System page to enable it.

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.

   File sharing appears to be properly configured.

7. Click **Support** > **Backup/Restore Database**. The Backup Database page opens as shown in the following example.



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**.

9. Click **Close** to close the progress window.

4. Delete the Database Snapshots

After you have saved the backup files, use the following instructions to delete the snapshots on the SMC and Flow Collector databases.

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

1. Log in to the SMC or Flow Collector console as **admin**.
2. **Check for Snapshots:** Type:

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

3. **Delete Snapshots (if they exist):** Type:

   ```
   /opt/vertica/bin/vsql -U dbadmin -w lan1cope -c "select
   remove_database_snapshot('StealthWatchSnap1');"
   ```

4. Repeat steps 1 through 3 to delete all saved SMC and Flow Collector database snapshots.

5. Re-enable SNMP Polling in the SMC

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

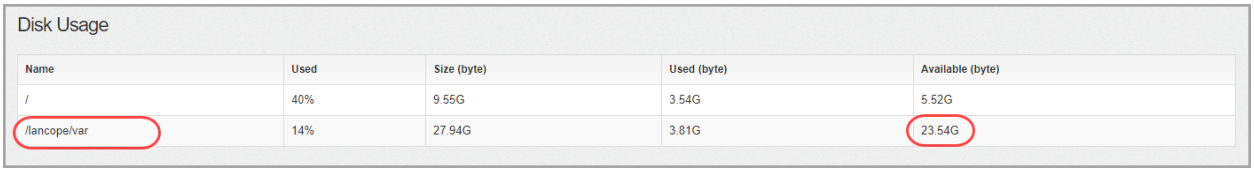
1. Return to the Desktop Client (but do not close the Appliance Admin interface).
2. Right-click the appropriate domain and select **Configuration** > **Exporter SNMP Configuration**. The Exporter SNMP Configuration page for that domain opens.
3. From the Default drop-down list, select the original entry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

6. Check the Available Disk Space

Check the disk space on the stand-alone 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.


Disk Usage

Name	Used	Size (byte)	Used (byte)	Available (byte)
/	40%	9.55G	3.54G	5.52G
/lancope/var	14%	27.94G	3.81G	23.54G

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.

7. Back Up the Update Log

Use these instructions to back up the update log in each stand-alone appliance.

1. SSH in to the appliance.
2. Log in as root.
3. Type the following:

```
cp /lancope/var/admin/upgrade/upgradeOutput.log /lancope/var/admin/upgrade/upgradeOutputHistory.log
```

4. Press Enter.
5. Exit the appliance.

> ⚠ Confirm you've completed procedures 1 through 7 on the appliance before you start the next procedure **8. Install Patches**.

8. Install Patches

Before you start the software update, make sure you install the latest patches on your appliances.

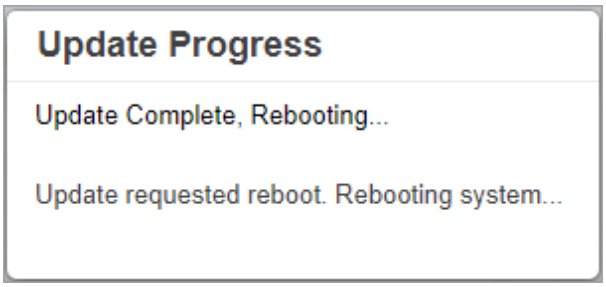
> ℹ Refer to the Patch Readme Notes for details.

1. **SMCs and Flow Collectors:** On the Admin Appliance **Home** page, review the **Uptime**. Make sure the appliance has been running for more than 1 hour and less than 7 days before you start the update.

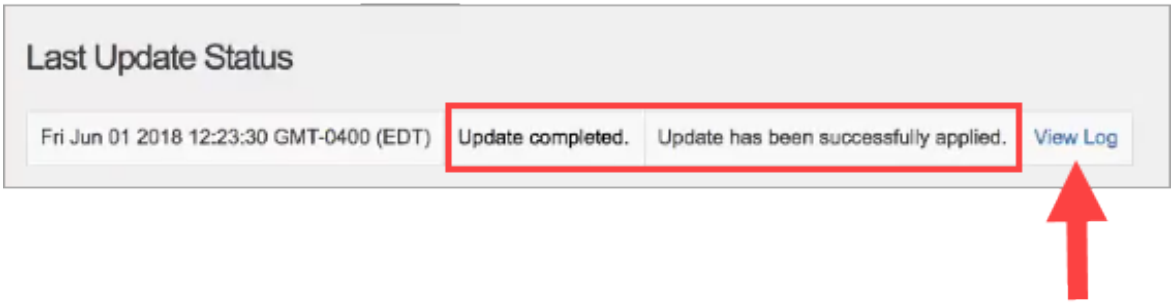
- If it is less than 1 hour, wait to proceed.
- If it is more than 7 days, click **Operations** > **Restart Appliance** to restart the appliance. Wait for at least 1 hour to confirm that all processes and safety checks are ready.

> ⚠ Do not restart the appliance while configuration changes are pending or if the configuration channel is down.

2. On the Admin Appliance **Support** > **Update** page.
3. Click **Choose File**.
4. Select the patch SWU file for the appliance.
5. Check the **Automatically Execute** check box.
6. 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.
7. When the Update Progress is shown as **complete** and **rebooting**, refresh the page.



8. Log in to the Appliance Admin interface.
9. **Confirm Installation:** Log in to the Appliance Admin interface.
10. Select **Support** > **Update**.
11. In the **Last Update Status** section, confirm the patch is shown as successfully applied. Click **View Log** for details.

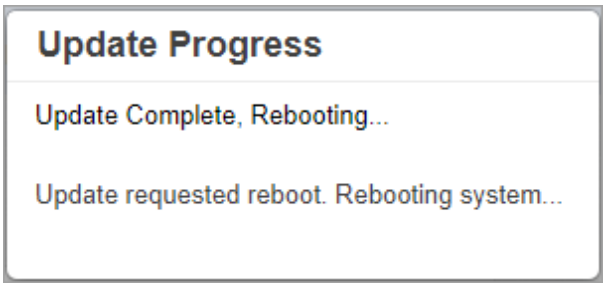


9. Install the v7.1.3 Software Update

1. **SMCs and Flow Collectors:** On the Admin Appliance **Home** page, review the **Uptime**. Make sure the appliance has been running for more than 1 hour and less than 7 days before you start the update.
   - If it is less than 1 hour, wait to proceed.
   - If it is more than 7 days, click **Operations** > **Restart Appliance** to restart the appliance. Wait for at least 1 hour to confirm that all processes and safety checks are ready.

> ⚠ Do not restart the appliance while configuration changes are pending or if the configuration channel is down.

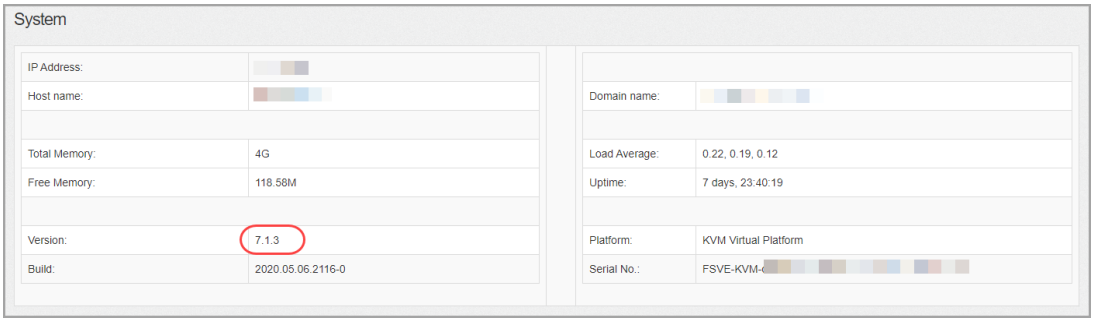
2. On the Admin Appliance **Support** > **Update** page. Click **Choose File**.
3. Select the v7.1.3 SWU file for the appliance.
4. Check the **Automatically Execute** check box.
5. Click **Upload**. Follow the on-screen prompts.
   - The upload progress is shown at the bottom of the page.
   - The safety checks and update may take several minutes.
6. When the Update Progress is shown as **complete** and **rebooting**, refresh the page.



> ⚠ Do not restart the appliance while configuration changes are pending or if the configuration channel is down. If the appliance is a Flow Collector, it may take up to 2 hours to complete the update. Review the **Best Time to Update: SMCs and Flow Collectors** section for details.

7. Log in to the Appliance Admin interface.
8. Review the software version shown on the Home page. Confirm the **Version** field shows v7.1.3.

   - **Reload:** If you have trouble loading any of the pages, clear your browser cache, close and re-open your browser, and log in again.
   - **Installation Failed** If the SWU installation failed, click **Support** > **Update**. Click **View Log**. Review the log for errors.
   - **Password Error:** Review the log for PASSHASH_ERROR. If the safety check found incompatible password hashing, refer to **Passwords** to reset your passwords.



10. 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.

- **Central 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.
- **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 and Stealthwatch Online Help.

Managed and Stand-Alone Requirements in Central Management

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

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

Order	Appliance	Central Management	Details
1.	Primary SMC	Managed	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.
2.	UDP Directors (also known as FlowReplicators)	Managed or Stand-Alone	
3.	Flow Collector 5000 Series Database	Managed	Make sure the Flow Collector 5000 series database is shown as Up before you start the engine configuration.
4.	Flow Collector 5000 Series Engine	Managed	Make sure the Flow Collector 5000 series database is shown as Up before you start the engine configuration.
5.	All Other Flow Collectors (NetFlow and sFlow)	Managed	
6.	Flow Sensors	Managed or Stand-Alone	Make sure your Flow Collector is shown as Up before you start the Flow

			Sensor configuration.
7.	Endpoint Concentrator	Stand-Alone	
8.	Secondary SMC (if used)	Managed	Make sure the primary SMC is shown as Up before you start the secondary SMC configuration.

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 **13. Update Stand-Alone 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 web: http://www.cisco.com/c/en/us/support/index.html
- To open a case by email: tac@cisco.com
- For phone support: 1-800-553-2447 (U.S.)
- For worldwide support numbers: https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

Copyright Information