



Cisco Secure Network Analytics

Update Guide 7.4.1



Table of Contents

Introduction	6
Overview	6
Audience	6
Terminology	6
What's New	7
Before You Begin	8
Software Version	8
Cisco Software Central	9
Licensing	9
Supported Hardware Platforms	9
CIMC Firmware Version	9
Apps Version Compatibility	10
VMware Version Compatibility	10
1. Review the VMware Version	11
2. Review the VMware Hosts	12
Compatible Browsers	13
Alternative Access	13
Server Identity Verification (7.3.x to 7.4.1 only)	14
Audit Log Destination Requirements	15
SMTP Configuration Requirements	15
Custom Certificates	16
Certificate Check	16
Cisco Bundles	16
Data Store	17
Expanding to a Data Store Environment with a New or an Existing Flow Collector ...	17
Data Store Private LAN Settings and Data Node Expansion	17
Identify Services Engine (ISE) or ISE-PIC	18
Cross-Site Request Forgery (CSRF) Protections (7.3.0 and 7.3.1 only)	19

Security Analytics and Logging (On Prem)	20
Report Builder	20
Disk Space	21
Host Name	21
Domain Name	21
NTP Server	22
Time Zone	22
Backing Up Your Appliances and Databases	22
sFlow Appliances in 7.4.0 and Earlier Releases	23
Best Time to Update	24
Software Update Files	24
All Appliances	24
SMCs (Managers) and Flow Collectors	24
Communications	25
Update Process Overview	26
1. Review Your Cluster	27
2. Download the Patches and the Update Files	28
1. Log in to Cisco Software Central	28
2. Download Patches	29
3. Download Update Files	30
SWU Files	30
3. Back Up the Appliance Configuration	32
4. Create a Diagnostics Pack	33
Creating a Diagnostics Pack in v7.3.x	33
Creating a Diagnostics Pack in v7.4.x	34
5. Back Up Databases for the SMC (Manager) and Flow Collector	35
1. Trim the Flow Collector Database	35
1. Review your Database Storage Statistics	35
2. Trim the Interface Details	36
3. Trim Flow Details and CI Event Data	37

2. Delete the Database Snapshots	37
3. Back Up to Remote File System	38
4. Delete the Database Snapshots	40
6. Back Up Data Store	42
1. Estimate Backup Host Storage Requirements	42
2. Install Python 3.7 and Rsync 3.0.5 on the Backup Host	43
3. Prepare the Backup Host	43
4. Enable Passwordless SSH Access for dbadmin	44
5. Initialize the Backup Directory on the Backup Host	45
6. Backup the Data Store Database	47
7. Check the Available Disk Space	48
8. Install Patches	50
1. Review the Installed Version	50
2. Install Required Patches	51
9. Install the v7.4.1 Software Update	55
Update Order	56
Install the Software Update	59
1. Upload the 7.4.1 SWUs	59
2. Install the 7.4.1 SWU	60
Troubleshooting	62
10. Configure High Availability	65
Primary Node and Secondary Node	65
Requirements	65
1. Configure the Primary UDP Director High Availability	66
2. Configure the Secondary UDP Director High Availability	67
Change History	69
11. Install the Desktop Client	70
Install the Desktop Client Using Windows	71
Install the Desktop Client Using macOS	73
12. Verify Manager (formerly SMC) Failover Roles	75

Introduction

Overview

Use this guide to update the following Cisco Secure Network Analytics (formerly Stealthwatch) appliances from version **7.3.x** (7.3.0, 7.3.1, and 7.3.2) or **7.4.0 to 7.4.1**:

- UDP Director (also known as Flow Replicator)
- Data Store



The update procedure for Data Nodes is unique in this update. Make sure you follow the instructions if you have a Data Store deployment.

- Flow Collector(s)
- SMC (which is renamed to Manager after updating to v7.4.x)
- Flow Sensor

In v7.4.0 we rebranded our Cisco Stealthwatch Enterprise products to Cisco Secure Network Analytics. For a complete list, refer to the [Release Notes](#). In this guide, you will see our former product name, Stealthwatch, used whenever necessary to maintain clarity, as well as terminology such as Stealthwatch Management Console and SMC.

Audience

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

Terminology

This guide uses the term “**appliance**” for any Secure Network Analytics (formerly Stealthwatch) product, including virtual products such as the Secure Network Analytics Flow Sensor Virtual Edition (VE).

A “**cluster**” is the group of appliances managed by the SMC (which is renamed to Manager after updating to v7.4.x). If an appliance is managed by the SMC (Manager), it is shown in your Central Management inventory.

What's New

For those already familiar with updating the system, make sure you are aware of the following changes since the last time you upgraded:

- Make sure to install the **Cisco Bundles** patch before beginning the update process.
- Make sure to update your **CIMC Firmware Version** before beginning the update process.
- Make sure the ISE certificate chain is complete before beginning the update process. See **Identify Services Engine (ISE) or ISE-PIC** for more information.
- Do not uninstall the Security Analytics and Logging (OnPrem) app. See **Security Analytics and Logging (On Prem)** for more information.
- Do not uninstall the Report Builder app. See **Report Builder** for more information.
- If you have more than one UDP Director, see **10. Configure High Availability**.
- We will run a **Server Identity Verification (7.3.x to 7.4.1 only)** as part of the update for SMTP Configuration and Audit Log Destination.
- If you're updating from v7.4.0, you no longer need to make sure the last appliance reboot for the Manager or Flow Collector was more than 1 hour and less than 7 days. However, if you're updating from v7.3.x, you will need to make sure the last reboot was more than 1 hour and less than 7 days.
- After the primary Manager is updated to v7.4.1, the appliance status in the Appliance Manager shows as **Connected** for all of the appliances that were successfully upgraded. The status for all appliances, including a secondary Manager, will show as **Up** until the primary Manager is updated. See **Communications** for more information.
- When updating a Data Node to v7.4.1, you don't need to install a patch SWU on each Data Node after the software update (as was required for v7.4.0).
- Make sure you select the correct SWU files based on whether you're upgrading from v7.3.x or v.7.4.0. The SWU files for v7.4.0 (and later) will have "v2" in the file names. See the **SWU Files** table to confirm which files you'll need for this update.



For more details about Secure Network Analytics v7.4.1, 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 will need to successfully update to v7.4.1.



Compliance Customers: If choosing to upgrade to v7.4.1, be advised this version includes a compliance violation. For FIPS and CC modes specifically, Secure Network Analytics TLS clients advertise non-compliant curves in the Supported Groups Extension of Client Hello messages, violating FCS_TLSC_EXT.1.4.

For more information, contact [Cisco Support](#).

Software Version

To update the appliance software to v7.4.1, the appliance must have **v7.3.x** (7.3.0, 7.3.1, or 7.3.2) or **v7.4.0** 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 Guides:** If you do not have Stealthwatch v7.3.x or v7.4.0 installed on your appliances, update them incrementally using the update guides on [Cisco.com](#). For example, if you have Stealthwatch v7.1.x installed, make sure you update each appliance from v7.1.x to v7.2.1, then v7.2.1 to v7.3.x, etc.
- **Patches:** As part of the update process, make sure to install the required rollup patches on your appliances.



Each required patch can take up to 90 minutes to install on each appliance.

- **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:** Secure Network Analytics requires TLS v1.2.
- **Third-Party Applications:** Secure Network Analytics does not support installing third-party applications on appliances.

Cisco Software Central

To manage your licenses, download patches, and download update files for Secure Network Analytics v7.4.1, log in to your Cisco Smart Account at <https://software.cisco.com> or contact your administrator.



To access patches or update files for Stealthwatch v7.1.3, continue to use the [Download and License Center](#).

Licensing

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

- **Check:** Log in to the SMC (Manager), then select the **Global Settings** icon > **Central Management** > **Smart Licensing**. Review the **Smart License Usage** section.
- **Instructions:** If any licenses are shown as Out of Compliance or Expired, refer to the [Smart Software Licensing Guide](#).

Supported Hardware Platforms

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

CIMC Firmware Version

The M4 common update process applies to UCS C-Series M4 hardware, and the M5 common update patch applies to M5 hardware, for the appliances shown in the following table.



Do not use the standard UCS firmware update information posted on Cisco.com.

M4 Hardware	M5 Hardware
SMC 2220 (Manager 2220)	SMC 2210 (Manager 2210)
FC 4200	FC 4210
FC 5020 Engine	---
FC 5020 Database	---

M4 Hardware	M5 Hardware
FC 5200 Engine	FC 5210 Engine
FC 5200 Database	FC 5210 Database
FS 1200	FS 1210
FS 2200	---
FS 3200	FS 3210
FS 4200	FS 4210
UD 2200	UD 2210

Follow the [2. Download Patches](#) instructions; but for step 3, select **Firmware** in the All Releases column to access the latest CIMC Firmware Version common update patches.

Go to the [Common Patch Readmes section on the Release Notes page](#) on cisco.com and locate the applicable readme for more details.

Apps Version Compatibility



If you have previously installed apps, make sure they are compatible with the version of Secure Network Analytics you will be installing.

To learn how to confirm the list of your installed apps and to see the latest Secure Network Analytics apps compatibility information, refer to the [Secure Network Analytics Apps Version Compatibility Matrix](#).

VMware Version Compatibility

Secure Network Analytics v7.4.x is compatible with VMware v6.5, v6.7, and v7.0. We do not support VMware v6.0 with Secure Network Analytics v7.4.x. For more information, refer to VMware documentation for vSphere 6.0 End of General Support.

- **Before the Update:** If your Secure Network Analytics appliances are installed on VMware v6.0, upgrade your VMware vCenter and ESXi hosts to v6.5, v6.7, or v7.0 before you upgrade Secure Network Analytics to v7.4.x.
- **Check:** Refer to [1. Review the VMware Version](#) and [2. Review the VMware Hosts](#) to review your VMware environment.

- **After the Update:** After the Secure Network Analytics v7.4.x update, there may be operating system errors shown in VMware. Review the VMware GUI and confirm your VMware vCenter is v6.5, v6.7, or v7.0 and the operating system is Debian v10. To upgrade the VMware vCenter or operating system, refer to your VMware guide.
- **Live Migration:** (for example, with vMotion) from host to host is not supported.
- **Snapshots:** Virtual machine snapshots are not supported.



Do not install VMware Tools on a Secure Network Analytics virtual appliance because it will override the custom version already installed. Doing so would render the virtual appliance inoperable and require re-installation.

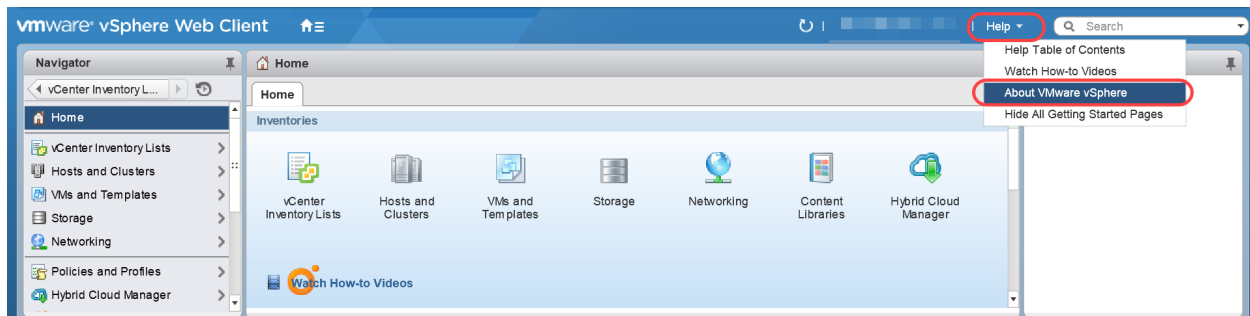
1. Review the VMware Version

Use the following instructions to confirm VMware vSphere vCenter has v6.5, v6.7, or v7.0 is installed.

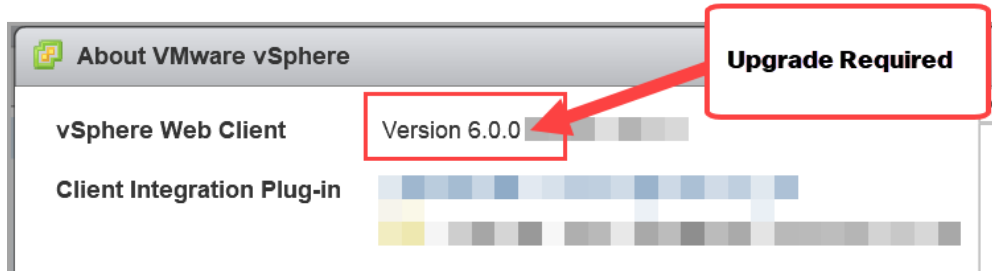


Some of the menus and graphics in the VMware UI can vary from the information shown here. Please refer to your VMware guide for details related to the software.

1. Log in to your VMware Web Client.
2. On the Home page, select **vCenter Inventory Lists**.
3. Select **Help > About VMware vSphere**.



4. Review the **Web Client** version. If it is v6.0, you need to upgrade it to v6.5, v6.7, or v7.0. Refer to your VMware guide for instructions.



5. Continue to the next section.

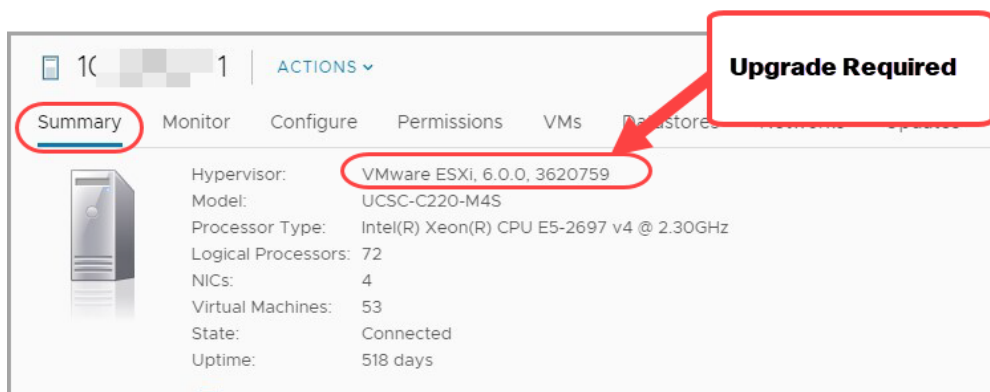
2. Review the VMware Hosts

Use the following instructions to review the ESXi host and confirm it has v6.5, v6.7, or v7.0 installed. If your Secure Network Analytics appliances are installed on more than one host, make sure you check each one.



Some of the menus and graphics in the VMware UI can vary from the information shown here. Please refer to your VMware guide for details related to the software.

1. In the Navigator pane, select **vCenter Inventory Lists**.
2. Select **Hosts**.
3. Click the host name.
4. Click the **Summary** tab.



5. Review the **Hypervisor** version. If it is v6.0, you need to upgrade it to v6.5, v6.7, or v7.0. Refer to your VMware guide for instructions.
6. Repeat steps 1 through 5 on any other hosts that have Secure Network Analytics appliances installed.

Compatible Browsers

- **Compatible Browsers:** Secure Network Analytics 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 Secure Network Analytics 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, refer to the [SSL/TLS Certificates for Managed Appliances Guide](#) to replace the certificate or contact [Cisco Support](#).

Alternative Access



It is important to enable an alternative way to access your Secure Network Analytics appliances for any future service needs.

Make sure you can access your Secure Network Analytics appliances using one of the following options:

Virtual Appliances - Console (serial connection to console port)

To access an appliance through **KVM**, refer to Virtual Manager documentation; or to connect to an appliance through **VMware**, refer to the vCenter Server Appliance Management Interface documentation for vSphere.

Hardware - Console (serial connection to console port)

To connect to an appliance using a laptop, or a keyboard with a monitor, refer to the latest [Secure Network Analytics Hardware Installation Guide](#) listed on the [Install and Upgrade Guides](#) page.

Hardware - CIMC (UCS appliance)

To access an appliance through CIMC, refer to the latest guide for your platform listed on the [Cisco Integrated Management Controller \(CIMC\) Configuration Guides](#) page.

Alternative Method

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

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



You will need to ensure SSH is enabled on all of your Data Nodes (by selecting the "Enable SSH" option) before upgrading or starting the database after a power outage. 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.

Use the following instructions to open and enable 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.
5. Locate the **SSH** section.
6. 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.
7. Click **Apply Settings**.
8. Follow the on-screen prompts to save your changes.



Make sure to disable SSH when you have finished using it.

Server Identity Verification (7.3.x to 7.4.1 only)

As part of the update from 7.3.x to 7.4.1, we will review the following configurations to confirm they meet the requirements for server identity verification:

- Audit Log Destination (Syslog over TLS)
- SMTP Configuration (email notifications for Response Management)

Review your configurations before you start the update. If your configurations do not meet the requirements, the update will fail.

Audit Log Destination Requirements

Make sure your Audit Log Destination configuration meets **both of the following requirements**:

- Confirm the root Certificate Authority (CA) SSL certificate from the syslog server that supports Syslog over TLS is included in your appliance trust store. Check each appliance trust store where you have Audit Log Destination configured.
- Also, if your syslog server identity certificate does not include the syslog server IP address in the Subject or Subject Alternative Name fields, add it to each appliance trust store where you have Audit Log Destination configured.

To access the trust stores, log in to the SMC (Manager), then select the **Global Settings** icon > **Central Management**. Click the **⋮ (Ellipsis)** icon for the appliance. Choose **Edit Appliance Configuration**. Select the **General** tab and scroll to the **Trust Store** section. For more information, refer to the [SSL/TLS Certificates for Managed Appliances Guide v7.3](#).

SMTP Configuration Requirements

Use **one of the following options** for server identity verification:

- Confirm your SMTP server identity certificate from your Certificate Authority (CA) has a Subject or Subject Alternative Name that matches the IP address or host name you have configured, **or**,
- Add the SMTP server identity certificate to the Trust Store.

To access the trust store, log in to the SMC (Manager), then select the **Global Settings** icon > **Central Management**. Click the **⋮ (Ellipsis)** icon for the SMC (Manager). Choose **Edit Appliance Configuration**. Select the **General** tab and scroll to the **Trust Store** section. For more information, refer to the [SSL/TLS Certificates for Managed Appliances Guide v7.3](#).

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 replace a custom appliance identity certificate, follow the instructions in the [SSL/TLS Certificates for Managed Appliances Guide](#) (v7.3 or v7.4).

Appliance Identity Requirements	
Format	PEM (.cer, .crt, .pem) or PKCS#12 (.p12, .pfx, .pks)
RSA Key Length	4096 bits or 8192 bits
Authentication	Server and client authentication are required for appliance identity certificates.

Certificate Check

If updating from v7.3.0, the update to v7.3.1, v7.3.2, and v7.4.0 includes a certificate check to verify the Cisco Bundles will not cause issues with your environment.

If you are using certificates, make sure the full chain of certificates (as separate files) is present in the Central Management Trust Store. If only the end-entity certificate is present in the Trust Store, the upgrade will fail.



If you do not have the full chain of certificates added to the Central Manager Trust Store, the update from Secure Network Analytics v7.3.0 will fail. If upgrading from v7.3.1 or v7.3.2, this check does not apply.

Cisco Bundles


Make sure you have the latest Cisco Bundles common update patch installed. For more information, refer to the readme for the [Cisco Bundles Common Update Patch](#). The patch:

- provides pre-validated digital certificates of a select number of root certificate authorities (CAs), and it
- includes a core certificate bundle and an external certificate bundle, which are used for connecting to Cisco services and to non-Cisco services.


Follow the **2. Download Patches** instructions; but for step 3, select **Certificate Bundles** in the Latest Release column to access the latest Cisco Bundles common update patch.

Data Store

If you have Data Store in your deployment, make sure SSH is enabled on all of your Data Nodes before you start the update.

 The "Last Status Change" and "Data Node Update Status" fields on the Data Store > Database Update tab in Central Management do not change following a rollup installation of a Data Node.

- **Enabling SSH:** Follow the steps in [Alternative Access](#) to enable SSH on all Data Nodes and be sure to select the **Enable SSH** checkbox instead of the Enable Root SSH Access option.
- **Disabling SSH:** If you want SSH to be disabled on your Data Nodes, you can disable SSH for each of your Data Nodes once the upgrade process and patch installation is complete.
- **Downtime:** If you're concerned about the downtime required for this update, please contact [Cisco Support](#).

 When updating a Data Node to v7.4.1, you don't need to install a patch SWU on each Data Node after the software update (as was required for v7.4.0).


Expanding to a Data Store Environment with a New or an Existing Flow Collector

Following an update to v7.4.1 (or later), you can expand you can expand your Secure Network Analytics non-Data Store environment by using an existing Flow Collector or by adding a new Flow Collector, and then adding the Data Node(s). Refer to the [Release Notes](#) and the instructions in the [System Configuration Guide](#) for more information. To understand how Secure Network Analytics Data Store works, review the [Data Store Solution Overview](#).

Data Store Private LAN Settings and Data Node Expansion


Starting with v7.4.1, Secure Network Analytics will be enforcing specific requirements for private LAN IP addresses. Make sure any Data Nodes configured using private LAN IP addresses meet these requirements:

- First three octets must be **169.254.42**
- Subnet must be **/24**


-  For example: 169.254.42.x/24 with the x representing a number (2 to 255) assigned by your site.

For more information, contact [Cisco Support](#).

Identify Services Engine (ISE) or ISE-PIC

-  Make sure the certificate chain in ISE is complete before you update to v7.4.1. Refer to the "Option 1 - Deploying Certificates Using ISE Internal Certificate Authority (Recommended)" section starting on page 5 of the [Cisco Secure Network Analytics ISE and ISE-PIC Configuration Guide 7.4](#) for details. Make sure to also correct any replication alarm issues in ISE by performing a manual sync. For additional information: See related ISE integration issues listed in the Known Issues section of the [Release Notes](#).

- **Requirement:** If your SMC (Manager) 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 (Manager) > **Client Group** column and check each SMC(Manager) in the list. If Cisco Adaptive Network Control (ANC) is not shown, check the SMC (Manager) check box to select it. Click **Group** to add ANC to the Group field, then click **Save**.

-  ANC is disabled by default, and it can only be enabled when pxGrid is enabled. To disable ANC once it has been enabled, make sure to manually disable the service through the Admin portal.

- **Guides:** Refer to the [Cisco Secure Network Analytics ISE and ISE-PIC Configuration Guide 7.4](#) and [Cisco Identity Services Engine Administrator Guide, Release 2.2](#) for more details. For additional product information about ISE, go to the [Cisco Identity Services Engine](#) page.

Cross-Site Request Forgery (CSRF) Protections (7.3.0 and 7.3.1 only)

If you are updating your system from v7.3.0 or v7.3.1 to v7.4.1, make sure you follow the steps in this section. If you are updating from v7.3.2 to v7.4.1, you can skip this section.

To help ensure more protection against CSRF attacks, the system requires HTTPS clients to submit CSRF tokens as part of their state-changing HTTPS requests. The CSRF token is session-specific and will be returned during authentication in a cookie called “XSRF-TOKEN.” HTTPS clients must set an HTTPS header “X-XSRF-TOKEN” to the value of this cookie when making HTTPS requests. As part of this added protection, your authentication API scripts might fail with HTTP 401 errors.

The steps to update your API scripts may vary depending on your environment. Before you update your cluster from v7.3.0 or v7.3.1 to v7.4.0, make sure you've made these changes to your API scripts:

1. When your HTTPS client(s) authenticate(s), store the CSRF token returned in the XSRF-TOKEN cookie.
2. On all HTTPS requests (with the exception of 'GET'), the script will need to return this stored value via an HTTP header called "X-XSRF-TOKEN".
3. Whenever the script re-authenticates, it will need to update the stored value of the CSRF token.



If you need to update your cluster before updating your API scripts, contact [Cisco Support](#).

Security Analytics and Logging (On Prem)



Do not uninstall the previous version of Security Analytics and Logging (OnPrem) or your existing data will be deleted.

After you've successfully updated to Secure Network Analytics v7.4.x, make sure to upgrade Security Analytics and Logging (OnPrem) to v3.1.0 . Previous versions of the app are not compatible with v7.4.x. If you don't upgrade, you won't be able to access Security Analytics and Logging (OnPrem). After you've downloaded the required file from Software Central, do the following to install Security Analytics and Logging (OnPrem):

1. Log in to your primary Manager.
2. Click the **Global Settings** icon.
3. Select **Central Management**.
4. Select the **App Manager** tab, and **Browse** for the file.
5. Follow the on-screen prompts to upload the file.

For more information about Security Analytics and Logging (OnPrem) deployment, refer to following documents:

- [Security Analytics and Logging \(On Premises\) Release Notes](#)
- [Getting Started with Cisco Security Analytics and Logging \(On Premises\)](#)
- [Security Analytics and Logging \(On Premises\): Firepower Event Integration Guide](#)

Report Builder



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

We moved Report Builder from a separate app to the core system in v7.4.0. If you are updating Secure Network Analytics from v7.3.x to v7.4.1, your app will be removed automatically as part of this update.

You do not need to uninstall your existing app. If you uninstall Report Builder, all files associated with it, including your saved reports and temporary files, are deleted. Do not delete the Report Builder app.

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. See [7. Check the Available Disk Space](#) for more information.

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

Host Name

- **Requirement:** 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:** Log in to the SMC (Manager), then select the **Global Settings** icon > **Central Management**. Check the Host Name column for each appliance.


Domain Name

- **Requirement:** A fully qualified domain name is required for each appliance. We cannot update an appliance with an empty domain.
- **Check:** Log in to the SMC (Manager), then 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**.

NTP Server

- **Requirement:** At least 1 NTP server is required for each appliance.
- **Check:** Log in to the SMC (Manager), then 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**.
- **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


 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.

All appliances use Coordinated Universal Time (UTC).

- **Requirement:** 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.

Backing Up Your Appliances and Databases

Make sure you plan time to back up your 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 Support](#).

 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 contact [Cisco Support](#).

This guide provides instructions for the following:

- Backing up each appliance
- Creating a diagnostics pack
- Backing up the SMC (Manager) database
- Backing up the Flow Collector(s) database
- Backing up Data Store

As part of the backup procedure you will delete database snapshots on the SMC (Manager) and Flow Collectors before, and then again after, you back up each database. Also, the procedure for backing up a Flow Collector includes trimming the database.

See [5. Back Up Databases for the SMC \(Manager\) and Flow Collector](#) for more information.



If you have a Data Store deployed, back up the Data Store database instead of the Flow Collector databases. See [6. Back Up Data Store](#) for more information.

sFlow Appliances in 7.4.0 and Earlier Releases

Starting in the 7.4.0 release, sFlow will not be released as a separate ISO image. You can toggle a Flow Collector NetFlow to sFlow. Refer to the "Advanced Settings" topic in the Online Help for more information.

Best Time to Update

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

Software Update Files

It takes time to download the patches and software update files. You can download them in advance. See [2. Download the Patches and the Update Files](#) for more information.

All Appliances

- **Time:** The patches for this update can take up to 90 minutes to install on each appliance. The software update process takes approximately 30 minutes to complete per appliance but can take longer depending on your network. These estimates do 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 (Managers) and Flow Collectors

- **Last Reboot/Active:** If you're updating from v7.3.x, make sure the SMC (Manager) 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. This reboot requirement does not apply to installing patches.
- **Flow Collectors** After a Flow Collector is updated and running, it will cache data to be sent to the SMC (Manager) until it 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.



Don't delete any Flow Collectors from Central Management. Doing so will cause the SMC (Manager) to lose all of the historical data for those Flow Collectors.

Communications

During the update process, communications will stop between the SMC (Manager) and the appliance while it updates and reboots.

In Central Management inventory, the appliance status changes to **Config Channel Down**. When the update is complete, communications are re-established and the appliance status returns to **Up**. See [9. Install the v7.4.1 Software Update](#) for more information.



Make sure the appliance status is shown as **Up** before you update the next appliance in your cluster.

Update Process Overview



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

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

- 1. Review Your Cluster**
- 2. Download the Patches and the Update Files**
- 3. Back Up the Appliance Configuration**
- 4. Create a Diagnostics Pack**
- 5. Back Up Databases for the SMC (Manager) and Flow Collector**
- 6. Back Up Data Store**
- 7. Check the Available Disk Space**
- 8. Install Patches**
- 9. Install the v7.4.1 Software Update**
- 10. Configure High Availability**
- 11. Install the Desktop Client**
- 12. Verify SMC (Manager) Failover Roles**

1. Review Your Cluster




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







Make sure to review your cluster to confirm the software version of each appliance. To verify that the current software version for each appliance is **7.3.x** (7.3.0, 7.3.1, or 7.3.2) or **v7.4.0** complete the following steps:

1. Log in to your SMC (Manager) as admin.

`https://<SMC IP address>`

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 to confirm each appliance has the same version of 7.3.x installed on all appliances.

Same Version: Make sure all appliances are using the same software version of 7.3.x. For example, if the SMC has 7.3.2 installed, the other appliances in your cluster also need to have 7.3.2 installed.

APPLIANCE TYPE	HOST NAME	IP ADDRESS	LAST REBOOT	INSTALLED VERSION	READY TO INSTALL	UPDATE STATUS	ACTIONS
SMC	smc01-10.205.99.9	10.205.99.9	2 hours ago	7.3.2 patch-smc-ROLLUP04-7.3.2-01	-		
SMC	smc02-10.205.99.10	10.205.99.10	2 hours ago	7.3.2 patch-smc-ROLLUP04-7.3.2-01	-		
Flow Collector	fc01-10.205.99.11	10.205.99.11	2 hours ago	7.3.2 patch-fcnf-ROLLUP05-7.3.2-01	-		
Flow Collector	fc02-10.205.99.12	10.205.99.12	2 hours ago	7.3.2 patch-fcsf-ROLLUP04-7.3.2-01	-		
UDP Director	udp01-10.205.99.13	10.205.99.13	19 hours ago	7.3.2 20210409.0329-58b668961ea	-		
Flow Sensor	fs-10.205.99.14	10.205.99.14	a month ago	7.3.2 20210409.0329-58b668961ea	-		



Once you start the update process, do not add or remove appliances, change your cluster configuration, change configuration settings on your appliances, or change the appliance failover roles.

2. Download the Patches and the Update Files

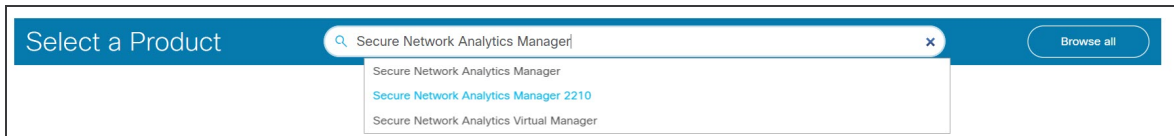
To manage your licenses, download patches, and download update files, log in to your Cisco Smart Account at <https://software.cisco.com>.

Use the following instructions to download patches and the v7.4.1 SWUs listed on your account.

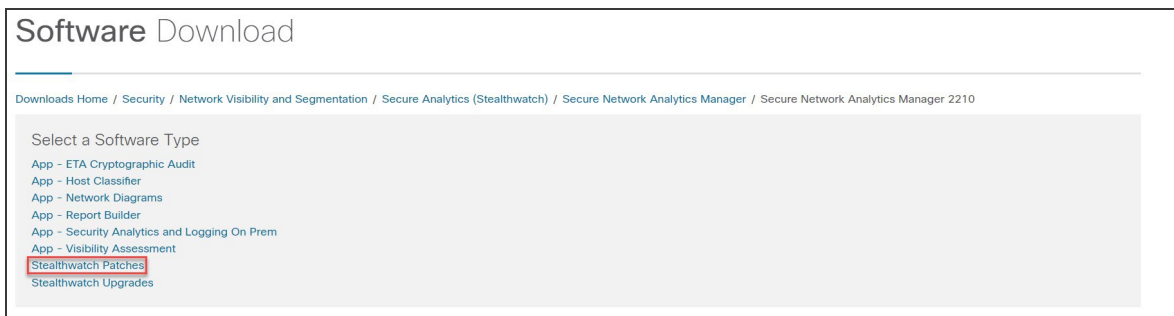
1. Log in to Cisco Software Central

1. Log in to Cisco Software Central at <https://software.cisco.com>.
2. On the Download and manage page in the **Download and Upgrade** section, select **Access downloads**.
3. Type **Secure Network Analytics** in the **Select a Product** field, then select an appliance.

You can also include the appliance when typing the product name, as in the following example:



4. When the Software Download page displays,
 - select **Stealthwatch Patches** to access any patch files you need to apply before beginning the update process



- or select **Stealthwatch Upgrades** to access the update files

Software Download

Downloads Home / Security / Network Visibility and Segmentation / Secure Analytics (Stealthwatch) / Secure Network Analytics Manager / Secure Network Analytics Manager 2210

Select a Software Type

- App - ETA Cryptographic Audit
- App - Host Classifier
- App - Network Diagrams
- App - Report Builder
- App - Security Analytics and Logging On Prem
- App - Visibility Assessment
- Stealthwatch Patches
- Stealthwatch Upgrades**

2. Download Patches



Select **Stealthwatch Patches** to access any patches you need to apply before beginning the update process. Refer to the [patch readmes](#) for more information.

After you select **Stealthwatch Patches**, the appliance page displays.

1. Select the version of Secure Network Analytics currently installed on your appliances. For example, if your appliances have 7.3.2 installed, select **7.3.2**.

Downloads Home / Security / Network Visibility and Segmentation / Secure Analytics (Stealthwatch) / Secure Network Analytics Manager / Stealthwatch Management Console 2200 / Stealthwatch Patches- 7.3.2

Search...

Expand All Collapse All

All Release

Certificate Bundles

Firmware

7.3

7.3.2

7.3.1

Stealthwatch Management Console 2200

Release 7.3.2

Related Links and Documentation

[My Notifications](#)

- No related links or documentation -

File Information	Release Date	Size	
7.3.2-PATCH SMC Rollup #5 patch-smc-ROLLUP005-7.3.2-01.swu	24-Aug-2021	2581.34 MB	Download Add to Cart Share

2. **Download:** Click the **Download** icon or **Add to Cart** icon.

Download all the patches for the selected appliance.



Make sure you download all of files for a the version, including appliance-specific rollup patches and common update patches, including CIMC Firmware Version and Cisco Bundles patches which apply to all appliances.

3. Repeat [these instructions](#) to download all patches for every appliance in your cluster. See the **SWU Files** table to confirm you have downloaded all required files for this update.

3. Download Update Files



The most efficient way to access all files for a specific version is to select the SMC (Manager) first.

After you select **Stealthwatch Upgrades**, the appliance page displays.

1. Select **7.4.1**.
2. **Download:** Click the **Download** icon or **Add to Cart** icon.
 - **Selected Appliance:** Download the update files shown for the appliance.
 - **Related Software:** Use the Related Software section to download the update files for all other appliances. If any patches are shown in this section, you will install them after the update.
3. See the **SWU Files** table to confirm you have downloaded all required files for this update. If you are missing any update files, repeat [these instructions](#) to download the update files for another appliance.

SWU Files

Confirm you have downloaded all required files for this update. If you are missing any files, see [2. Download the Patches and the Update Files](#) .



There may be a later patch rollup number on Cisco Software Central than the number shown here. Make sure you download and install the latest patch.

Appliance	Updating from v7.3.x Software Update File Name	Updating from v7.4.0 Software Update File Name
UDP Director (also known as Flow Replicator) UDP Director VE (also known as Flow Replicator VE)	update-udpd- 7.4.1.20220411.1352- 0674092e2d2e-0-01.swu	update-udpd- 7.4.1.20220411.1352- 0674092e2d2e-0-v2-01.swu
Data Node	update-dnode- 7.4.1.20220411.1352- 0674092e2d2e-0-01.swu	update-dnode- 7.4.1.20220411.1352- 0674092e2d2e-0-v2-01.swu

Appliance	Updating from v7.3.x Software Update File Name	Updating from v7.4.0 Software Update File Name
Flow Collector database 5000 series	update-fcdb- 7.4.1.20220411.1352- 0674092e2d2e-0-01.swu	update-fcdb- 7.4.1.20220411.1352- 0674092e2d2e-0-v2-01.swu
Flow Collector (NetFlow) (This is needed for the Flow Collector 5000 series engine) Flow Collector (NetFlow)VE	update-fcnf- 7.4.1.20220411.1352- 0674092e2d2e-0-01.swu	update-fcnf- 7.4.1.20220411.1352- 0674092e2d2e-0-v2-01.swu
Flow Collector (sFlow) Flow Collector (sFlow) VE	update-fcsf- 7.4.1.20220411.1352- 0674092e2d2e-0-01.swu	update-fcsf- 7.4.1.20220411.1352- 0674092e2d2e-0-v2-01.swu
Flow Sensor Flow Sensor VE	update-fsuf- 7.4.1.20220411.1352- 0674092e2d2e-1-01.swu	update-fsuf- 7.4.1.20220411.1352- 0674092e2d2e-1-V2-01.swu
SMC (Manager) SMC (Manager) VE	update-smc- 7.4.1.20220411.1352- 0674092e2d2e-0-01.swu	update-smc- 7.4.1.20220411.1352- 0674092e2d2e-0-v2-01.swu

3. Back Up the Appliance Configuration


Without a backup, you will not be able to recover your files if a problem occurs during the update process. These steps are important to help minimize data loss.

 Make sure to back up each appliance configuration.

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 (Manager).
 - **All Managed Appliances:** To back up the configuration of all appliances managed by the Central Manager, select your primary SMC (Manager).
 - **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**.
7. Continue to [4. Create a Diagnostics Pack](#)

SMC (Manager) and Central Manager: When you back up your primary SMC (Manager) and Central Manager, there will be a SMC (Manager) backup configuration file and a Central Management backup configuration file.

 If you are backing up the SMC (Manager) and Flow Collector, make sure to also back up the databases. You need both backups to restore these appliances completely. For more information about backing up your SMC (Manager) and Flow Collector databases, see [5. Back Up Databases for the SMC \(Manager\) and Flow Collector](#).

4. Create a Diagnostics Pack

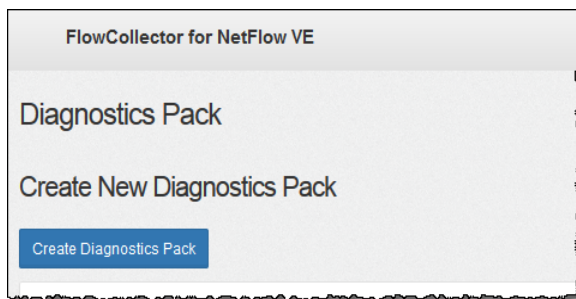
Having a diagnostics pack can be invaluable if you need to work with [Cisco Support](#) to troubleshoot an issue. Follow the instructions for your version of Secure Network Analytics:

- **v7.3.x: [Creating a Diagnostics Pack in v7.3.x](#)**
- **v7.4.0: [Creating a Diagnostics Pack in v7.4.x](#)**

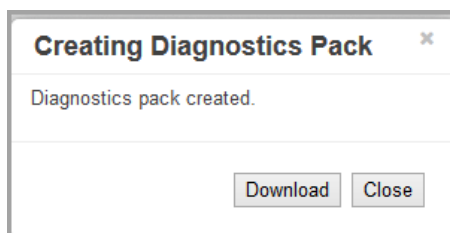
Creating a Diagnostics Pack in v7.3.x

Create a diagnostics pack for each appliance using Appliance Administration:

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 can 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`.

Creating a Diagnostics Pack in v7.4.x

Create a diagnostics pack for each appliance using System Configuration:

1. Log in to the appliance console as root.
2. Type `SystemConfig`. Press Enter.
3. Select **Recovery**.
4. Select **Diagnostics Pack**.
5. To customize your diagnostics pack, select a menu and click **Edit**.

Menu	Description
File Name Prefix	Add a file name prefix for your diagnostics pack (maximum of 127 characters).
Password	Create a file password for your diagnostics pack. If you do not create a file password, we will encrypt the diagnostics pack with the default method (Cisco key).
Configuration Backup	Select this option and follow the on-screen prompts to include a configuration backup in your diagnostics pack. For more information about backups, refer to Backup Configuration Files in the Help.
Modules	Edit the diagnostic pack contents by selecting the specific modules you want to include.

6. Click **Finish**. Follow the on-screen prompts to create the diagnostics pack.

5. Back Up Databases for the SMC (Manager) and Flow Collector



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. Also note that this procedure only applies to Non-Data Store Flow Collectors. For assistance, contact [Cisco Support](#).

After creating a diagnostics pack for the SMC (Manager) and Flow Collector(s), make sure to back up the databases. For assistance, contact [Cisco Support](#).

This process involves completing the following procedures:

1. **Trim the Flow Collector Database**
2. **Delete the Database Snapshots**
3. **Back Up to Remote File System**
4. **Delete the Database Snapshots**

1. Trim the Flow Collector Database

The Flow Collector database backup can 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 /lancope/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).

The screenshot shows the Stealthwatch GUI with the following sections:

- Database Storage Statistics - Capacity Table:**

	Average	Work
Capacity in Days	50	49
Remaining Days	22	21
Bytes Per Day	549.46M	563
- Flow Data Summary Table:**

Data	Days	Containers	Total	Average Per Day	Largest Day	Total
Flow Details	28	32	148.75M	5.31M	5.49M	3.4
Flow Interface Details	14	20	213.3M	15.24M	16.65M	5.9
Total	28	52	362.05M	20.55M	21.15M	9.4
- CI Event Data Summary Table:**

Data	Days	Containers	Total	Average Per Day	Largest Day	Total
CI Events	28	29	351.17k	12.54k	12.85k	8.53M
CI Event Details	28	29	351.17k	12.54k	12.85k	4.06M
Total	28	58	702.34k	25.08k	25.71k	12.59M

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. This function uses the Desktop Client as a main tool which does not apply to Data Store systems. A node may be needed to indicate that the trimming procedure only applies to Non-Data Store systems.

The screenshot shows the 'Quick View for Flow' window with the following table:

Exporter	Exporter Type	Interface	Direction	TTL	DSCP	Flow Action
Cisco	Cisco	#Index-2	Outbound			Permitted
Cisco	Cisco	#Index-3	Inbound			Permitted

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 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 and CI Event/Details in the Flow Collector database, contact [Cisco 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.

2. Delete the Database Snapshots

Before you create backup files, make sure you delete any saved snapshots on the SMC (Manager) and Flow Collector databases using the following instructions.



Make sure you delete the SMC (Manager) and Flow Collector database snapshots. This step is critical for a successful backup.

1. Log in to the SMC (Manager) and Flow Collector appliance database console as **admin**.
2. **Check for Snapshots:** Type:

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

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

```
/opt/vertica/bin/vsql -U dbadmin -w lanlcope -c "select remove_
database_snapshot('StealthWatchSnap1');"
```

4. Wait until the snapshot folder is removed: Check:

```
ls /lancope/var/database/dbs/sw/v_sw_node0001_data/Snapshots/
```

If the results are not empty, continue to wait. You may need to wait several minutes until the folder is removed, depending on the size of the database.

- Repeat steps 1 through 4 to delete all saved SMC (Manager) and Flow Collector database snapshots.

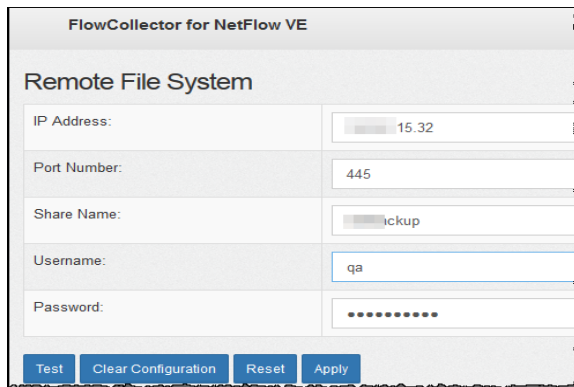
3. Back Up to Remote File System

To back up a 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.
- Return to the Appliance Admin interface (but do not close the Desktop Client).
 - 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.

Name	Used	Size (byte)	Used (byte)	Available (byte)
/	37%	4.92G	1.68G	2.99G
/lancope/var	68%	37.03G	24.48G	11.79G

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



The screenshot shows the 'Remote File System' configuration page. The title is 'FlowCollector for NetFlow VE'. Below the title is the section header 'Remote File System'. There are five input fields: 'IP Address' with the value '15.32', 'Port Number' with the value '445', 'Share Name' with the value 'backup', 'Username' with the value 'qa', and 'Password' which is masked with dots. At the bottom of the form are four buttons: 'Test', 'Clear Configuration', 'Reset', and 'Apply'.

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

The 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.

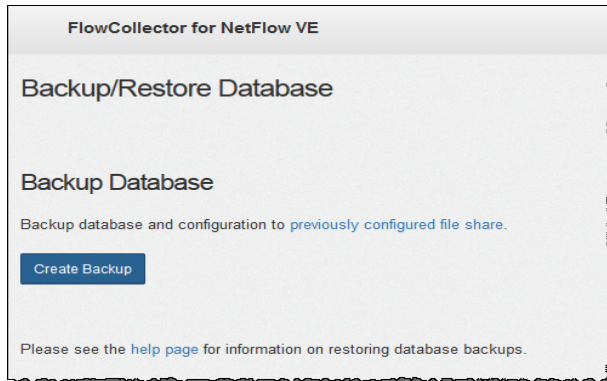
If the Apply button is not enabled after you enter the password, click once in a blank area on the Remote File System page to enable it.

6. Click **Test** to verify that the 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.



If you cancel the backup before it finishes, make sure you delete the database snapshots again. See [4. Delete the Database Snapshots](#) for detailed instructions.

4. Delete the Database Snapshots

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



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

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

```
/opt/vertica/bin/vsql -U dbadmin -w lanlcope -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. Wait until the snapshot folder is removed: Check:

```
ls /lancope/var/database/dbs/sw/v_sw_node0001_data/Snapshots/
```

If the results are not empty, continue to wait. You may need to wait several minutes until the folder is removed, depending on the size of the database.

5. Repeat steps 1 through 4 to delete all saved SMC (Manager) and Flow Collector database snapshots.

6. Back Up Data Store

i If you're new to having Data Store, contact Cisco Professional Services for assistance with planning and implementing these tasks.

Refer to the [Data Store Hardware Deployment and Configuration Guide](#) or [Data Store Virtual Edition Deployment and Configuration Guide](#) for more information on Data Store database backup.

To backup your Data Store, you must complete the following:

- 1. Estimate Backup Host Storage Requirements**
- 2. Install Python 3.7 and Rsync 3.0.5 on the Backup Host**
- 3. Prepare the Backup Host**
- 4. Enable Passwordless SSH Access for dbadmin**
- 5. Initialize the Backup Directory on the Backup Host**
- 6. Backup the Data Store Database**

1. Estimate Backup Host Storage Requirements

To estimate the size of the backup, do the following:

1. Log in to your Data Node's console as `root`.
2. Copy the following command, paste it into the command line, and press Enter to connect to the database using `vsq1` and execute the query. Enter your password when prompted. Note the results.

```
/opt/vertica/bin/vs1 -U dbadmin -c "SELECT SUM(used_bytes)
FROM storage_containers;"
```

i Make sure the backup host has at least twice the storage capacity of the backup size.

3. Multiply the sum by 2 to estimate how much storage space your backup host needs.

i Based on the estimated storage requirements, identify a host running Linux on your network to store the backup, or deploy a host running Linux with the necessary storage requirements. Use a Linux-based host separate from your Stealthwatch appliances.

2. Install Python 3.7 and Rsync 3.0.5 on the Backup Host

Make sure you're using a Linux-based host separate from your Stealthwatch appliances, then install Python 3.7 and rsync 3.0.5 on the backup host:

1. Log in to the backup host console as `root`.
2. From the command prompt, enter `python --version` and press Enter to see what version of Python you have installed.
 - If Python 3.7 is not installed, continue to step 3.
 - If Python 3.7 is already installed, skip to step 5.
3. Enter `sudo apt-get update` and press Enter to download updated versions of packages, including Python. Enter your password when prompted.
4. Enter `sudo apt-get install python3.7` and press Enter to install Python 3.7.
5. From the command prompt, enter `rsync -version` and press Enter to see what version of rsync you have installed.
 - If rsync 3.0.5 is not installed, continue to step 6.
 - If rsync 3.0.5 is already installed, go to **3. Prepare the Backup Host**.
6. Enter `sudo apt-get update` and press Enter to download updated versions of packages, including rsync. Enter your password when prompted.
7. Enter `sudo apt-get install rsync` and press Enter to install rsync.

3. Prepare the Backup Host

To prepare a backup host, do the following:

1. Log in to the backup host console as `root`, if not already logged in.
2. From the command prompt, enter `getent passwd | grep dbadmin` and press Enter to determine if a `dbadmin` user account exists on this host:
 - If the `dbadmin` user account does not exist, then make sure to create a `dbadmin` user account on this host. Continue to step 3.
 - If a `dbadmin` user account already exists, the backup host is ready. Go to **4. Enable Passwordless SSH Access for dbadmin**.
3. From the command prompt, enter `useradd dbadmin` and press Enter to create a `dbadmin` user account.
4. Enter `passwd dbadmin` and press Enter to assign a password to `dbadmin`.
5. Enter a **New password** and press Enter to set the `dbadmin` password.
6. Confirm the password when prompted.

4. Enable Passwordless SSH Access for dbadmin

To enable passwordless SSH access for the `dbadmin` user account, do the following:

1. Log in to the backup host console as `root`, if not already logged in.
2. Open port 22/TCP between the backup host and each Data Node for SSH, and port 50000/TCP between the backup host and each Data Node for rsync.
3. Review the OpenSSH documentation on `ssh-copy-id` for more information.
4. Log in to the first Data Node as `root`.
5. Copy the following command and paste it into a plain text editor:

```
ssh-copy-id -i dbadmin@[hostname]
```

6. Replace `[hostname]` with the backup host's hostname.
7. Copy the updated command, paste it into the command prompt, and press Enter to copy the `dbadmin` SSH authorized key to the backup host.
8. Copy the following command and paste it into a plain text editor:

```
ssh 'dbadmin@[hostname]'
```

9. Replace `[hostname]` with the backup host's hostname.
10. Copy the updated command, paste it into the command prompt, then press Enter to verify that you can log in to the remote host's console over SSH without needing a password from this Data Node.



Make sure you're able to log in to the remote host's console over SSH without a password.

5. Initialize the Backup Directory on the Backup Host

To initialize the backup directory on the backup host, do the following:

1. Log into the first Data Node's console as `root`.
2. From the command prompt, enter `python --version` and press Enter to see what version of Python you have installed.

i Make a note of the Data Node you use to initialize the backup directory because you will use the same Data Node when you backup to database (in **6. Backup the Data Store Database**).

3. Enter `su - dbadmin` and press Enter to run the following commands as the `dbadmin` user.
4. Copy the following command to a text editor: `ssh [backup-host-ip]`
5. Replace `[backup-host-ip]` with your backup host's IP address.
6. Copy the updated command, paste it in the command prompt, and press Enter to verify that you can log into the backup host's interface as `dbadmin` without being prompted for a password. If the backup host prompts you for a password, check your settings.
7. Enter `cd /home/dbadmin` and press Enter to change directories.
8. Enter `mkdir backups` and press Enter to create the `backups` directory.
9. Enter `exit` and press Enter to return to the Data Node's command line prompt.
10. Enter `vi pw.ini` and press Enter to create the `pw.ini` backup password file, and edit it.

i If you update the `dbadmin` password using the `setup-sw-datastore-secure-connectivity` script, you must also update the password stored in the `pw.ini` backup password file, or your backup fails.

11. Copy the following lines to a plain text editor:

```
[Passwords]
dbPassword = [dbadmin-password]
```

12. Update `[dbadmin-password]` to the Data Store `dbadmin` password.
13. Copy the updated lines and paste them into the `pw.ini` backup password file.
14. Press Esc, then enter `:wq`, then press Enter to exit and save your changes.

15. Enter `chmod 640 pw.ini` and press Enter to change the `pw.ini` file permissions to allow the `dbadmin` user to read and edit the file.
16. Enter `vi config.ini` and press Enter to create the `config.ini` backup configuration file and edit it.
17. Copy the following lines and paste them into a plain text editor:

```
[Mapping]
v_sw_node0001 = backup-host-ip:/home/dbadmin/backups
v_sw_node0002 = backup-host-ip:/home/dbadmin/backups
v_sw_node0003 = backup-host-ip:/home/dbadmin/backups
```

```
[Misc]
snapshotName = data_store_backup
passwordFile = /home/dbadmin/pw.ini
enableFreeSpaceCheck = True
retryCount = 2
retryDelay = 1
```

```
[Transmission]
encrypt = true
checksum = true
concurrency_backup = 2
concurrency_restore = 2
```

18. Replace `backup-host-ip` with the backup host's IP address.
19. If the host names under `[Mapping]` do not match your Data Nodes, update the host names.



Make sure you have an entry for each Data Node if you deployed more than three to your environment.

20. Copy the updated lines and paste them into the `config.ini` file.
21. Press Esc, then enter `:wq`, then press Enter to exit and save your changes.
22. Enter `vbr -t init -c config.ini` and press Enter to initialize the `/home/dbadmin/backups` directory on the backup host to receive Data Store backups.

6. Backup the Data Store Database

1. Log in as `root` to the console of the same Data Node you used to initialize the backup host directory (as you noted in the first step of **5. Initialize the Backup Directory on the Backup Host**).
2. Enter `su - dbadmin` and press Enter to run the following commands as the `dbadmin` user.
3. Enter `vbr -t backup -c config.ini --debug 3 --dry-run` and press Enter to perform a test of the backup without creating the backup:
 - If the backup test resolves successfully, back up the Data Store. Continue to step 4.
 - If the backup test fails to resolve, review the debug log files in the `/tmp/vbr` directory and resolve the root cause, then test the backup again.

 Contact [Cisco Support](#) for assistance if you cannot resolve the issue.

4. Enter `vbr -t backup -c config.ini` and press Enter to backup the Data Store to the `/home/dbadmin/backups` directory on the backup host.
5. Continue to **7. Check the Available Disk Space**.

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 (Manager) for all appliance SWU files that you upload to Update Manager. Also, confirm you have enough available space on each individual appliance.

- **SMC (Manager):** When the SWU is uploaded to the Update Manager in Central Management, it will use additional space on the SMC (Manager) during the update. The file remains on the SMC (Manager) in Central Management until it is replaced by another file of the same type.

Make sure you have enough available space on the SMC (Manager) 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 (Manager) 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.

Use these instructions to confirm you have enough available disk space to install patches and software update files on the SMC (Manager) 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 four times the size of the individual software update file (SWU) available. On the SMC (Manager), you need at least four 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 (/lancope/var) partition (1 SWU file x 6 GB x 4 = 24 GB available).
- **SMC (Manager):** For example, if you upload four SWU files to the SMC (Manager) that are each 6 GB, you need at least 96 GB available on the /lancope/var partition (4 SWU files x 6 GB x 4 = 96 GB available).

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, refer to the Data Storage section of the [installation guide](#) for your appliance.
6. Repeat steps 1 through 5 to check the available space on each appliance.

8. Install Patches

Before you start the software update, make sure you install the latest patches on your appliances. To download patches, see [2. Download the Patches and the Update Files](#) for details.




Confirm you've completed procedures 3 through 7 on every managed appliance in your cluster before you install patches.

When installing patches, we recommend you follow these best practices:

- **Readme:** You can upload an update patch SWU file for a specific appliance, or upload a common update patch which will apply to all appliances in Central Management. For details about a specific update patch, refer to the readme located on cisco.com.
- **Order:** Make sure you install patches on the appliances in the order specified in this section. For this update, you will install the rollup patch on your **secondary** SMC (Manager) first.
- **Time:** These patches can take up to 90 minutes to install on each appliance. Do not reboot the appliance while configuration changes are pending or if the configuration channel is down.
- **Confirm:** Confirm the patch is installed and that each appliance status is shown as **Up** before you start the next patch installation.

1. Review the Installed Version

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

1. Log in to your primary SMC (Manager).
2. Click the  (**Global Settings**) icon.
3. Select **Central Management**.
4. Review the **Appliance Status** column and confirm each appliance is shown as **Up**.
5. Select the **Update Manager** tab, and locate the **System Updates** section.
6. Review the **Installed Version** column. Confirm each appliance is consistent, with only version **7.3.x** (7.3.0, 7.3.1, or 7.3.2) or **7.4.0** installed.

This example shows the Installed Version for all appliances is v7.3.2.

System Updates ●							
APPLIANCE TYPE	HOST NAME	IP ADDRESS	LAST REBOOT	INSTALLED VERSION	READY TO INSTALL	UPDATE STATUS	ACTIONS
SMC	smc01-10.200.99.9	10.200.99.9	2 hours ago ●	7.3.2 patch-smc- ROLLUP004-7.3.2-01	-		⊕
SMC	smc02-10.200.99.10	10.200.99.10	2 hours ago ●	7.3.2 patch-smc- ROLLUP004-7.3.2-01	-		⊕
Flow Collector	fcnf-10.200.99.11	10.200.99.11	2 hours ago ●	7.3.2 patch-fcnf- ROLLUP005-7.3.2-01	-		⊕
Flow Collector	fcfs-10.200.99.12	10.200.99.12	2 hours ago ●	7.3.2 patch-fcsf- ROLLUP004-7.3.2-01	-		⊕
UDP Director	udp01-10.200.99.13	10.200.99.13	19 hours ago ●	7.3.2 20210409.0329-58b6668961ea	-		⊕
Flow Sensor	fs-10.200.99.14	10.200.99.14	a month ago ●	7.3.2 20210409.0329-58b6668961ea	-		⊕

2. Install Required Patches

Make sure to install any required **v7.3.x** (v7.3.0, v7.3.1, or v7.3.2) or **v7.4.0** patches before updating to v7.4.1.

Use the following instructions to install the latest rollup patch on your SMC (Manager)s. If you have two SMCs (Managers) configured for failover, install the patch on the secondary SMC (Manager) before the primary SMC (Manager).



Install the patch on the **secondary** SMC (Manager) and confirm the installation is finished before you install the patch on the primary SMC (Manager).

On the **Update Manager** page:

1. Click **Upload**.
2. Select the SMC (Manager) latest rollup patch SWU file.
3. In the **Update Manager > System Updates** section, check the **Ready to Install** column for your SMCs (Managers) and confirm the patch is shown.
4. Click the **Actions** menu for the secondary SMC (Manager).

Primary SMC (Manager): If you've already finished the patch installation on the secondary SMC (Manager), click the **Actions** menu for the primary SMC (Manager).

5. Select **Install Update**.
6. Follow the on-screen prompts to confirm the update.

- **Update Status:** The update status column will change from Waiting to Install... to Installing.
- **Reboot:** The appliance reboots automatically.

Not all patches reboot the appliance. Do not reboot the appliance while changes are in progress.



The patch can take up to 90 minutes to install on each appliance. 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.


7. Confirm Installation:

- Click the **Actions** menu for the SMC (Manager).
- Select **View Update Log**.
- Confirm the patch is listed as successful or installed. If the patch was unsuccessful, correct any errors and try again. For more information, see [Troubleshooting](#).

8. Review the SMC (Manager) on the **Central Management > Appliance Manager** page. Confirm the appliance status is shown as **Up**.

9. If you have two SMCs (Managers) configured for failover, repeat steps 4 through 8 to install the patch on the primary SMC (Manager).

10. Repeat these steps for all other appliances in your cluster, in the following order:

Order	Appliance	Notes
1.	All UDP Directors (also known as Flow Replicators)	If you have a High Availability cluster, install the patch on the secondary UDP Director first.
2.	All Data Nodes or Flow Collector 5000 Series Database	<div style="border: 1px solid #00a0e3; padding: 5px;">  Your cluster will not have both Data Nodes and Flow Collector 5000 Series Database. </div>

		<p>Data Nodes</p> <p>Apply the patch to every Data Node in your Data Store. Wait for Central Management to show all Data Node appliance statuses as Up before proceeding.</p> <p>Flow Collector 5000 Series Database</p> <p>Make sure the Flow Collector series database completes the patch installation and the appliance status is shown as Up before you start the engine update.</p>
3.	Flow Collector 5000 Series Engine	Make sure the Flow Collector series database completes the patch installation and the appliance status is show as Up before you start the engine update.
4.	All Other Flow Collectors (NetFlow and sFlow)	Make sure the Flow Collector completes the patch installation and the appliance status is shown as Up before you install the patch on the next appliance in your cluster.
5.	Flow Sensors	

11. Confirm Installation:

- Click the **Actions** menu for the SMC (Manager).
- Select **View Update Log**.
- Confirm the patch is listed as successful or installed. If the patch was unsuccessful, correct any errors and try again. For more information, see [Troubleshooting](#).

12. In the **Update Manager > System Updates** section, check the **Ready to Install** column for each appliance and confirm the rollup patch is shown.



The patch can take up to 90 minutes to install on each appliance. Do not reboot the appliance while configuration changes are pending or if the configuration channel is down. To confirm the appliance status as **Up**, review the Central Management > Appliance Manager page.

9. Install the v7.4.1 Software Update

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



Make sure your SMC (Manager) and Flow Collector(s) have been running for more than 1 hour and less than 7 days before you start the software update (if you're updating from v7.3.x).


When installing the software update, we recommend you follow these best practices:

- **Order:** Make sure you update the appliances in order and review the details in the [Update Order](#) section before you start.
- **Wait:** If you're updating from v7.3.x, make sure your SMCs and Flow Collectors have been running for more than 1 hour and less than 7 days before you start the 7.4.1 software update.
- **Confirm:** Confirm the update is installed and that each appliance status is shown as **Up** before you begin the next appliance update.
- **Multiple Appliances:** With the exception of SMCs (Managers), Flow Collector 5000s, UDP Directors in high availability (HA), and Data Nodes, 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](#).
- **Data Store:** If you have a Data Store deployed, make sure SSH is enabled on all of your Data Nodes (by selecting the "Enable SSH" option), which is required before upgrading or starting the database after a power outage.

Follow the steps in [Alternative Access](#) to enable SSH on all of your Data Nodes, and be sure to select the **Enable SSH** checkbox instead of the Enable Root SSH Access option. If you want SSH to be disabled on your Data Nodes, you can go back and disable SSH for each of your Data Nodes once the upgrade process is complete.

Update Order

Update your appliances in the following order:


Order	Appliance	Notes
1.	UDP Directors (also known as Flow Replicators)	<p>If you have a High Availability cluster, update the secondary UDP Director first.</p> <p>Confirm the update is completed and the secondary UDP Director appliance status is shown as Up before you update the primary UDP Director.</p>
2.	All Data Nodes or Flow Collector 5000 Series Database	<div style="border: 1px solid #00a0e3; padding: 10px; margin-bottom: 10px;"> <p> Your cluster will not have both Data Nodes and Flow Collector 5000 Series Database.</p> </div> <p>Data Nodes</p> <p>Before you start the update, make sure SSH is enabled on each Data Node. Refer to Data Store in the Introduction for more information.</p> <p>Flow Collector 5000 Series Database</p> <p>Make sure the Flow Collector series database completes the update and the appliance status is shown as Up before you start the engine update.</p>
3.	Flow Collector 5000 Series Engine	<p>Make sure the engine update is completed and the appliance status is shown as Up before you update the next appliance in your cluster.</p>
4.	All Other Flow Collectors (NetFlow and sFlow)	<p>Make sure the Flow Collector has been running for more than 1 hour and less than 7 days before you start the</p>

		<p>update (if you're updating from v7.3.x).</p> <p>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.</p>
5.	Flow Sensors	<p>Upload the Flow Sensor SWU file. If you're upgrading from v7.3.x, the appliance status for the Flow Sensor may display as Config Changes Pending.</p>
6.	Secondary SMC (Manager) *if used	<p>Make sure the SMC (Manager) has been running for more than 1 hour and less than 7 days before you start the update (if you're updating from v7.3.x).</p> <p>If your system uses a secondary SMC (Manager) confirm the secondary SMC (Manager) update is completed and confirm the secondary SMC (Manager) appliance status is shown as Up before you start the primary SMC (Manager) update.</p> <p>After the update completes, both SMCs (Managers) may restart in the secondary role. If this occurs, refer to 12. Verify Manager (formerly SMC) Failover Roles for details. Do not change the failover roles until both SMCs (Managers) are updated.</p>
7.	Primary SMC (Manager)	<p>Make sure the SMC (Manager) has been running for more than 1 hour and less than 7 days before you start the update (if you're updating from v7.3.x).</p>


		<p>If your system uses a secondary SMC (Manager), confirm the secondary SMC (Manager) update is completed and confirm the secondary SMC (Manager) appliance status is shown as Up before you start the primary SMC (Manager) update.</p> <p>After the update completes, both SMCs (Managers) may restart in the secondary role. If this occurs, refer to 12. Verify Manager (formerly SMC) Failover Roles for details. Do not change the failover roles until both SMCs (Managers) are updated.</p>
--	--	---


Install the Software Update

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

 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.







1. Upload the 7.4.1 SWUs

1. Log into your SMC (Manager).
2. Type `https://<SMC IP address>` in your browser address bar.
3. Click the  (**Global Settings**) icon.
4. Select **Central Management**.
5. 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.

6. Review the **Installed Version** column. Confirm each appliance has the same version of 7.3.x installed (**7.3.0**, **7.3.1** or **7.3.2**) or **7.4.0**.

This example shows that all appliances have the same installed version, 7.3.2. Note that all appliances have the same installed version.

APPLIANCE TYPE	HOST NAME	IP ADDRESS	LAST REBOOT	INSTALLED VERSION	READY TO INSTALL	UPDATE STATUS	ACTIONS
SMC	smc001-10-200-99-9	10.200.99.9	2 hours ago	7.3.2 patch-smc- ROLLUP004-7.3.2-01	-		
SMC	smc002-10-200-99-10	10.200.99.10	2 hours ago	7.3.2 patch-smc- ROLLUP004-7.3.2-01	-		
Flow Collector	fc001-10-200-99-11	10.200.99.11	2 hours ago	7.3.2 patch-fcnf- ROLLUP005-7.3.2-01	-		
Flow Collector	fc002-10-200-99-12	10.200.99.12	2 hours ago	7.3.2 patch-fcsf- ROLLUP004-7.3.2-01	-		
UDP Director	udp001-10-200-99-13	10.200.99.13	19 hours ago	7.3.2 20210409.0329-58b668961ea	-		
Flow Sensor	fs-10-200-99-14	10.200.99.14	a month ago	7.3.2 20210409.0329-58b668961ea	-		


7. Click **Upload**.
8. Follow the on-screen prompts to select a SWU file. Upload one file at a time.
 - **Updates:** Upload a SWU file for each appliance type in Central Management.
 - **Flow Sensors:** Upload the Flow Sensor SWU file after you update the SMCs (Managers).
 - **Disk Space:** See [7. Check the Available Disk Space](#) for more information.

2. Install the 7.4.1 SWU

Use the following instructions to update the software using Central Management.

 Make sure you update the [appliances in order and you follow the notes](#).

1. Select the **Appliance Manager** tab. Confirm the appliance status for all appliances is shown as **Up**.
2. Select the **Update Manager** tab.
3. Review the **System Updates** section. Check the following columns for the appliance to confirm it is ready to update:
 - **Ready to Install:** Confirm that the **7.4.1** SWU file is posted. If the **Flow Sensor** SWU file is not posted, [upload](#) it after you update your SMC (Manager).
 - **Last Reboot of SMCs (Managers) and Flow Collectors:** Make sure the last reboot was more than 1 hour and less than 7 days (if you're updating from v7.3.x).
 - 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.

4. Click the **Actions** menu for the appliance.
5. Select **Install Update**.
6. 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 once per 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.

7. Check the **Installed Version** column to confirm it shows the version **7.4.1** software update.
 - **Installation Successful:** If **7.4.1** is shown as the Installed Version for the appliance, continue to the next step to confirm the appliance status.
 - **Installation Failed:** If the Update Status column shows "Install Failed," click the **Actions** menu > **View Update Log** for details. If you can resolve the issue, try the update again. For more information, see [Troubleshooting](#).
8. Select the **Appliance Manager** tab. Locate the appliance in the inventory.
 - **Up or Connected:** Confirm the appliance status is shown as **Up**. After you install the primary Manager, the appliance status shows as **Connected** for all successfully installed appliances.
 - **Primary Manager:** Confirm the Appliance Status for your primary Manager is shown as **Connected**. The secondary Manager status remains as **Up** until the primary Manager is updated. Then, the status for all appliances shows as **Connected**.
9. Repeat all steps in this section, [2. Install the 7.4.1 SWU](#), for the next appliance. Make sure you update the appliances in order.
10. If you've updated every appliance in Central Management to v7.4.1, go to [10. Configure High Availability](#) (UDP Directors only). If you do not have UDP Directors in your deployment, go to [11. Install the Desktop Client](#).

Troubleshooting

Error Description or Category	Details
Install Update button is unavailable	<p>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. If the appliance is a Flow Sensor, upload the SWU file after you update your SMCs (Managers).</p> <p>Also, check the Last Reboot column to confirm the last reboot on your SMCs (Managers) and Flow Collectors was more than 1 hour and less than 7 days (if you're updating from v7.3.x).</p> <ul style="list-style-type: none"> • 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 (Manager) and the managed appliances	<p>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 Installation and Configuration Guide for instructions.</p> <p>Retry the patch or software update file installation after you confirm network connectivity is restored.</p>
Failed: We couldn't match this file with the digital signature. Try to upload the file again. If the problem persists, please contact Cisco Support.	<p>Confirm that you have the correct SWU. If you're unable to determine whether you have the correct SWU, contact Cisco Support.</p>
No space left on device (Disk Space)	<p>Check the disk space on each appliance to confirm you have enough available space to install patches and software update files.</p>

Error Description or Category	Details
	<p>On each managed appliance, you need at least 4 times the size of the individual software update file (SWU) available. On the SMC (Manager), you need at least 4 times the size of all appliance SWU files that you upload to Update Manager.</p> <ul style="list-style-type: none"> • Managed Appliances: For example, if the Flow Collector SWU file is 6 GB, you need at least 24 GB available on the Flow Collector (/lancope/var) partition (1 SWU file x 6 GB x 4 = 24 GB available). • SMC (Manager): For example, if you upload four SWU files to the SMC (Manager) that are each 6 GB, you need at least 96 GB available on the /lancope/var partition (4 SWU files x 6 GB x 4 = 96 GB available). • Additional Information: See 7. Check the Available Disk Space for more information.
Unexpected exit status!	<p>If you encounter this error, it may be the following:</p> <ul style="list-style-type: none"> • a service failed to stop cleanly during the installation preparation • the update was started before meeting the reboot requirements <p>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 Installation and Configuration Guide for instructions.</p> <p>Also, check the Last Reboot column to confirm the last reboot on your SMCs (Managers) and Flow Collectors was more than 1 hour and less than 7 days (if you're updating from v7.3.x).</p> <ul style="list-style-type: none"> • If it is less than 1 hour, wait to proceed.


Error Description or Category	Details
	<ul style="list-style-type: none"> 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.
<p>SIVR-CHECK Warning! We found certificate validation issues that will break the following integrations.</p>	<p>Your Audit Log Destination or SMTP Configuration configurations did not meet the requirements for server identity verification. See Server Identity Verification (7.3.x to 7.4.1 only) for more information. Correct your configurations and try the update again.</p>
<p>Upload Failed</p>	<p>Make sure you upload one file at a time. We do not support uploading multiple SWU files at the same time.</p> <p>Confirm each upload is completed and shown in the Ready to Install column before you start uploading another SWU file. See 9. Install the v7.4.1 Software Update for more information.</p>




If you cannot resolve the error, contact [Cisco Support](#).

10. Configure High Availability

If you have more than one UDP Director, use the Appliance Admin interface to configure high availability.

-  High Availability is only available on UDP Director hardware appliances. High Availability is not available on virtual appliances.

The UDP Director High Availability (HA) allows a user to configure settings for redundant UDP Directors. Both nodes are fully redundant, however only one node is online at a time.

-  If you have high availability configured on your UDP Directors and update Secure Network Analytics to v7.4.0 or later, make sure to reconfigure high availability after the update using **1. Configure the Primary UDP Director High Availability**.

Primary Node and Secondary Node

The online node is known as the Primary in the pair, while the offline node is the Secondary. If the Primary node in the pair should fail, the Secondary node takes over and becomes the Primary

Requirements

- **Forwarding Rules:** Configure at least one [forwarding rule](#) for the UDP Director in the High Availability system.
- **Save the Rules Configuration File:** If the UDP Director has already been configured with rules, export (save the rules configuration file) the UDP Director rules. Then, import the file to the second UDP Director to ensure that the rules for each match.
- **Order:** Configure the Primary UDP Director and then repeat the configuration on the Secondary one.
- **New or Established:** If the both UDP Directors are new, make sure you follow the procedures for each in this guide. However, if the secondary is already configured as an appliance on the Secure Network Analytics system, log in to the secondary UDP Director and configure its High Availability components as described here.

1. Configure the Primary UDP Director High Availability

1. Log in to the primary UDP Director.
2. Click **Configuration > High Availability**.

Check the **Enable High Availability Service** check box for the High Availability Settings.

<input type="checkbox"/> Enable High Availability Service	
High Availability Settings	
Node ID	<input type="radio"/> 1 <input type="radio"/> 2
Virtual IP Address	<input type="text"/>
Subnet Mask	<input type="text"/>
Shared Secret	L@n <input type="password"/> IHA
Sync Ring #1(eth2) Unicast IP Address	<input type="text"/>
Sync Ring #1(eth2) Subnet Mask	<input type="text"/>
Sync Ring #2(eth3) Unicast IP Address	<input type="text"/>
Sync Ring #2(eth3) Subnet Mask	<input type="text"/>
Paired Node Host Name	<input type="text"/>
Paired Node Sync Ring #1(eth2) IP Address	<input type="text"/>
Paired Node Sync Ring #2(eth3) IP Address	<input type="text"/>

3. Select your **Node ID**. If this is a primary UDP Director, select 1. If this a secondary UDP Director, select 2.
4. In the **Virtual IP Address** field, enter an unused IP address that is on the same subnet as the eth0 interface. Set the **Subnet Mask** value to the value of the subnet mask used on the eth0 interface.



Make sure the Virtual IP Address is the same on both nodes.

5. In the **Shared Secret** field, type a string for both UDP Directors. (This will be encrypted for secure transfer.)

6. In the fields for **Sync Ring #1 (eth2) Unicast IP Address**, enter the IP address and the subnet mask. (A Unicast IP Address identifies a single network destination.)
7. In the fields for **Sync Ring #2 (eth3) Unicast IP Address**, enter the IP address and the subnet mask.
8. Each of the IP addresses--eth0, eth02, eth03--must be on its own separate unicast subnet. In the **Paired Node Sync Ring #1(eth2) IP Address** field, enter the Eth2 IP address for the secondary UDP Director.
9. In the **Paired Node Host Name** field, enter the host name for the secondary UDP Director.
10. In the **Paired Node Sync Ring #1(eth2) IP Address** field, enter the Eth2 IP address for the secondary UDP Director.
11. In the **Paired Node Sync Ring #1(eth3) IP Address** field, enter the Eth3 IP address for the secondary UDP Director.
12. After reviewing the setting, click **Apply** to set the configuration.
13. Continue to the next section to configure the second UDP Director of the cluster.

2. Configure the Secondary UDP Director High Availability



If you selected Node ID 2 in [step 4](#) above, complete these steps for the primary UDP Director.

To configure the secondary UDP Director complete the following steps:

1. Log in to the secondary UDP Director.
2. Click **Configuration > High Availability**.
3. Enter the host name for the secondary UDP Director into the **Paired Node Host Name** field.
4. Configure all of the parameters on this screen (including any Advanced Parameters that you may have changed on the first appliance) exactly as you did on the first appliance with exactly same values for every field except for the following:
 - **Sync Ring #1(eth2) Unicast IP Address:** Enter a different IP address from what you configured in this field on the primary, but it must be in the same subnet as the Sync Ring 1 Unicast address given on the primary.
 - **Sync Ring #2(eth3) Unicast IP Address:** Enter a different IP address from what you configured in this field on the primary, but it must be in the same subnet as the Sync Ring 2 Unicast address given on the primary.

- **Paired Node Host Name:** Enter the host name for the primary UDP Director in this field.
 - **Paired Node Sync Ring #1(eth2) IP Address:** Enter the Eth2 IP address for the primary UDP Director in this field.
 - **Paired Node Sync Ring #1(eth3) IP Address:** Enter the Eth3 IP address for the primary UDP Director in this field.
5. Click **Apply** to save your changes and to start the clustering services on this appliance.
 6. Click **Promote** to designate the primary appliance.
 7. **Restart:** Select **Operations > Restart Appliance**.

Change History

Revision	Revision Date	Description
1_0	April 18, 2022	Initial version.
1_1	May 9, 2022	General Availability (GA).
1_2	August 5, 2022	Updated note related to Data Nodes in the Introduction section. Updated the SWU filenames.
1_3	November 1, 2022	Added a note to the Data Store section.
1_4	December 12, 2022	Modified note in the Data Store section.

11. Install the Desktop Client



Starting with v7.4.0, the SMC has been renamed to Manager. The SMC is referred to as Manager within this section.



If your Secure Network Analytics system is deployed with only Data Store Flow Collectors, you will not use the Desktop Client. For a hybrid Data Store/Non-Data Store system, the Desktop Client will only work with Non-Data Store domains.

The following information applies to installing and using the Desktop Client:

- You can locally install different versions of Desktop Client.
- The Desktop Client includes Stealthwatch terminology such as Stealthwatch Management Console and SMC (Manager).
- If you want to access multiple versions of Desktop Client, you will need a different executable file for each Manager.
- If you are using both a primary and a secondary Manager, you will need to log off one Manager before you can log in to the other Manager.
- You can have different versions of Desktop Client open simultaneously.
- When you update to a later version of Secure Network Analytics, you will need to install the new version of Desktop Client.
- Use the Web App to monitor and configure your Secure Network Analytics installation if you deploy a Data Store. The Desktop Client is incompatible with a Data Store.

Instructions for installing the Desktop Client vary depending on whether you're using Windows or macOS:

- [Install the Desktop Client Using Windows](#)
- [Install the Desktop Client Using macOS](#)

You will also change memory size differently, depending on whether you're using Windows or macOS:

- [Change the Memory Size From Windows Explorer](#)
- [Change the Memory Size From Finder](#)


Install the Desktop Client Using Windows

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


Use the following instructions to install the Desktop Client using Windows:

1. Log in to your Manager.
2. Click the **Download** icon.



3. Click the .exe file to begin the installation process.
4. Follow the steps in the wizard to install the Desktop Client.
5. On your desktop, click the Desktop Client icon .
6. In the **SMC Server Name** field, enter the Manager server name or IP address (IPv4 or IPv6).
7. Enter the Manager user name and password.
8. Follow the on-screen prompts to open the Desktop Client and trust the appliance identity certificate.

Change the Memory Size From Windows Explorer

-  You can change how much Random Access Memory (RAM) to allocate on your client computer to run the 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 Desktop Client for the first time.)

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

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

```
# Enter one VM parameter per line# Use -Xms to specify the initial Java heap size and Use -Xmx to specify the maximum heap size-Xms512m-Xmx2048m
```

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

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

```
# Enter one VM parameter per line# Use -Xms to specify the initial Java heap size and Use -Xmx to specify the maximum heap size-Xms512m-Xmx2048m
```

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

- If you notice that the 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 Desktop Client.
- Desktop Client requires a 64-bit operating system. It cannot run on a 32-bit operating system or Linux.

Use the following instructions to install the Desktop Client using macOS:

1. Log in to your Manager.
2. Click the **Download** icon.



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

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



4. Drag the Desktop Client icon (🍏) into the Application folder.

The icon is added to the Launchpad.

5. On your desktop, click the Desktop Client icon (🍏).
6. In the **SMC Server Name** field, enter the Manager server name or IP address (IPv4 or IPv6).
7. Enter the Manager user name and password.
8. Follow the on-screen prompts to open the Desktop Client and trust the appliance identity certificate.

Change the Memory Size From Finder



You can change how much Random Access Memory (RAM) to allocate on your client computer to run the 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 Desktop Client for the first time.)

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

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

```
# Enter one VM parameter per line# Use -Xms to specify the initial Java heap size and Use -Xmx to specify the maximum heap size-Xms512m-Xmx2048m
```

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.

```
# Enter one VM parameter per line# Use -Xms to specify the initial Java heap size and Use -Xmx to specify the maximum heap size-Xms512m-Xmx2048m
```

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

- If you notice that the 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 Manager (formerly SMC) Failover Roles



Reminder: Starting with v7.4.0, the SMC has been renamed to Manager. The SMC is referred to as Manager within this section.



Do not change the failover roles until both Managers are updated.



Do not add or remove appliances from Central Management until you have finished the failover configuration and confirmed the secondary Manager's Appliance Status is shown as **Connected** in Central Management.

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

1. Log into the **secondary** Manager as an admin user.
2. Click the **Global Settings** icon.
3. Select **Manager Configuration**.
4. Click the **Failover Configuration** tab.
5. Confirm the **Failover Role** is shown as **Secondary**.

The screenshot shows the 'Manager Configuration' interface. The 'Failover Configuration' tab is active. A blue informational banner at the top states: 'Make sure you add all required certificates to your Manager Trust Stores. Also, configure the secondary Manager before the primary Manager. For instructions, please refer to [Help](#).' Below this, the 'Failover Role*' dropdown menu is highlighted with a red box and shows 'Secondary' selected. At the bottom, the 'Other Manager' section shows 'IP Address*' as '141' and 'Failover Role' as 'Primary'.

6. Log in to the **primary** Manager. Follow steps 2 through 4 to confirm the **Failover Role** is shown as **Primary**.
7. If both Managers are shown as secondary, change the failover roles so you have one primary Manager and one secondary Manager. Make sure you follow the configuration order and instructions in the [Failover Configuration Guide](#).



For instructions, refer to the [Failover Configuration Guide](#).

8. Log in to the **secondary Manager**.
9. Review the Flow Collection Trend.



10. **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 Manager.

- Log in to the primary Manager.
- Click the **Global Settings** icon. Select **Central Management**.
- On the Appliance Manager page, locate the Flow Collector.
- Click the **⋮ (Ellipsis)** icon.
- Select **Reboot Appliance**. Follow the on-screen prompts.
- **Flow Collectors:** Repeat these steps to reboot every Flow Collector in Central Management.
- **Secondary Manager:** Repeat these steps to reboot your secondary Manager.

11. Log in to the primary Manager.
12. Review the **Central Management > Appliance Manager**. Confirm the secondary Manager Appliance Status is shown as **Connected**.

Contacting Support

If you need technical support, please do one of the following:

- Contact your local Cisco Partner
- Contact Cisco Support
- To open a case by web: <http://www.cisco.com/c/en/us/support/index.html>
- To open a case by email: tac@cisco.com
- For phone support: 1-800-553-2447 (U.S.)
- For worldwide support numbers:
<https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html>

Copyright Information

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)

