



Cisco Secure Network Analytics

Update Guide 7.5.0



Table of Contents

Introduction	5
Overview	5
Audience	5
Terminology	5
What's New	6
Before You Begin	7
Software Version	7
Cisco Software Central	7
Smart Licensing	8
Smart Licensing Transport Configuration	8
Supported Hardware Platforms	8
CIMC Firmware Version	8
Apps Version Compatibility	9
Security Analytics and Logging (On Prem)	9
Analytics	10
VMware Version Compatibility	10
1. Review the VMware Version	10
2. Review the VMware Hosts	11
Compatible Browsers	12
Alternative Access	13
Certificate Validity	14
Cisco Bundles	14
Data Store	15
Data Store Private LAN Settings and Data Node Expansion	15
Identify Services Engine (ISE) or ISE-PIC	15
Disk Space	16
Host Name	16
Domain Name	17

NTP Server	17
Time Zone	17
Backing Up Your Appliances and Databases	17
MongoDB Upgrade	18
Best Time to Update	19
Software Update Files	19
All Appliances	19
Managers and Flow Collectors	19
Communications	20
Update Process Overview	21
1. Review Your Cluster	22
2. Download the Patches and the Update Files	23
1. Log in to Cisco Software Central	23
2. Download Patches	24
3. Download Update Files	25
SWU Files	26
3. Back Up the Appliance Configuration	27
4. Create a Diagnostics Pack	28
5. Back Up Databases for the Manager and Flow Collector	30
1. Trim the Flow Collector Database	30
1. Review your Database Storage Statistics	30
2. Trim the Interface Details	31
3. Trim Flow Details and CI Event Data	32
2. Delete the Database Snapshots	32
3. Back Up to Remote File System	33
4. Delete the Database Snapshots	35
6. Back Up Data Store	37
1. Estimate Backup Host Storage Requirements	37
2. Prepare a Backup Host	37
3. Enable Passwordless SSH Access for dbadmin	39

4. Initialize the Backup Directory on the Backup Host	39
5. Back Up the Data Store Database	42
Data Store Backup Failure	42
7. Check the Available Disk Space	43
8. Install Patches	45
1. Review the Installed Version	45
2. Install Required Patches	46
9. Install the v7.5.0 Software Update	50
Update Order	51
Install the Software Update	54
1. Upload the 7.5.0 SWUs	54
2. Install the 7.5.0 SWU	55
Troubleshooting	58
10. Configure High Availability	60
Primary Node and Secondary Node	60
Requirements	60
1. Configure the Primary UDP Director High Availability	61
2. Configure the Secondary UDP Director High Availability	62
11. Install the Desktop Client	64
Install the Desktop Client Using Windows	65
Install the Desktop Client Using macOS	67
12. Verify Manager Failover Roles	69
Contacting Support	71
Change History	72

Introduction

Overview

Use this guide to update the following Cisco Secure Network Analytics (formerly Stealthwatch) appliances from version **7.4.0**, **7.4.1**, **7.4.2** to **7.5.0**:

- 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)
- Flow Sensor
- Manager

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 product, including virtual products such as the Secure Network Analytics Flow Sensor Virtual Edition (VE).

Additionally, a “**cluster**” is the group of appliances managed by the Manager. If an appliance is managed by the Manager, it is shown in your Central Management inventory.



For more details about Secure Network Analytics v7.5.0, refer to the [Release Notes](#).

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:

- We have improved the performance of upgrades, refreshes, and factory resets.
- We have changed the transport configuration requirements for Smart Licensing. Confirm that the appliance is able to connect to smartreceiver.cisco.com.
- Make sure all appliances in your system meet the [baseline requirement](#) of 1 month (30 days) before beginning the update process.
- There are new CPU instruction set requirements for VE deployments in v7.5.0. Ensure that your CPU is capable of the AVX/AVX2 instruction sets. For ESXi, select a VM hardware version of 11 or greater. For KVM, we recommend that you utilize host passthrough.
- Make sure to upload *all* SWU files before you begin installing any of the SWU files.
- Note that after the primary Manager upgrades successfully, the appliance status in the Appliance Manager shows as **Connected** for *all* of the appliances that have upgraded successfully. See [Communications](#) for more information.
- Make sure to install the [Cisco Bundles](#) patch and 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 details.
- When upgrading from v7.4.1 to v7.5.0, your Analytics data is not carried over. Analytics data from v7.4.2 will be carried over to v7.5.0. For more details about Analytics, refer to [Analytics: Detections, Alerts, and Observations](#).
- During the update, we will upgrade MongoDB to v6.0.9. See [MongoDB Upgrade](#).
- If you have more than one UDP Director, see [10. Configure High Availability](#).
- If you have v7.4.1 or later installed on your Data Nodes, follow the instructions to use the **Update all Data Nodes** button to update your Data Nodes at the same time. Make sure you restart Vertica on any Data Node after the update SWU file is successfully installed on **all** Data Nodes.
- After you update the system to 7.5.0, the root user access and Appliance Setup Tool are removed. Refer to the [Release Notes](#) for details.

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 v7.5.0.

Software Version

To update the appliance software to v7.5.0, the appliance must have version **7.4.0**, **7.4.1**, or **7.4.2** 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:

- **Baselining:** Before you start this update, make sure your appliances have been running on the same version of **v7.4.0**, **v7.4.1**, or **v7.4.2** for more than 1 month (30 days). If you've updated your system to more than one version in a short period of time, your system baselining may be impacted. For assistance, please contact [Cisco Support](#).
- **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. Following an upgrade to v7.5.0, TLS v1.2 and TLS v1.3 will both be supported by default. Refer to the [SSL/TLS Certificates for Managed Appliances Guide](#) for instructions.
- **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 v7.5.0, log in to your Cisco Smart Account at <https://software.cisco.com> or contact your administrator.

Smart Licensing

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

- **7.4.0, 7.4.1 Check:** Log in to the Manager. Select the **Global Settings** icon > **Central Management** > **Smart Licensing**. Review the **Smart License Usage** section.
- **7.4.2 Check:** Log in to the Manager. Select **Configure** > **GLOBAL 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](#).

Smart Licensing Transport Configuration

We have changed the transport configuration requirements for Smart Licensing.



If you are upgrading the appliance from v7.4.1 or earlier, make sure that the appliance can connect to smartreceiver.cisco.com.

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, the M5 common update patch applies to M5 hardware, and the M6 common update patch applies to M6 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	M6 Hardware
SMC 2200 (Manager 2200)	SMC 2210 (Manager 2210)	SMC 2300 (Manager 2300)
FC 4200	FC 4210	FC 4300
FC 5020 Engine	---	---
FC 5020 Database	---	---

M4 Hardware	M5 Hardware	M6 Hardware
FC 5200 Engine	FC 5210 Engine	---
FC 5200 Database	FC 5210 Database	---
FS 1200	FS 1210	FS 1300
FS 2200	---	---
FS 3200	FS 3210	FS 3300
FS 4200	FS 4210 / FS 4240	FS 4300
UD 2200	UD 2210	---
---	DS6200	DN6300

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](#).

Security Analytics and Logging (On Prem)

After you've successfully upgraded to Secure Network Analytics v7.5.0, make sure to upgrade Security Analytics and Logging (OnPrem) to v3.3.0. 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](#)

Analytics

When upgrading from v7.4.1 to v7.5.0, your Analytics data is not carried over. Analytics data from v7.4.2 will be carried over to v7.5.0. For more details about Analytics, refer to [Analytics: Detections, Alerts, and Observations](#).

VMware Version Compatibility

Secure Network Analytics v7.5.x is compatible with VMware v7.0 or v8.0. We do not support VMware v6.0, v6.5, or v6.7, with Secure Network Analytics v7.5.x. For more information, refer to VMware documentation for vSphere 6.0, 6.5, and 6.7 End of General Support.

- **Before the Update:** If your Secure Network Analytics appliances are installed on VMware v6.0, v6.5, or v6.7, upgrade your VMware vCenter and ESXi hosts to v7.0 or v8.0 before you upgrade Secure Network Analytics to v7.5.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 v7.5.x update, there may be operating system errors shown in VMware. Review the VMware GUI and confirm your VMware vCenter is v7.0 or v8.0 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.

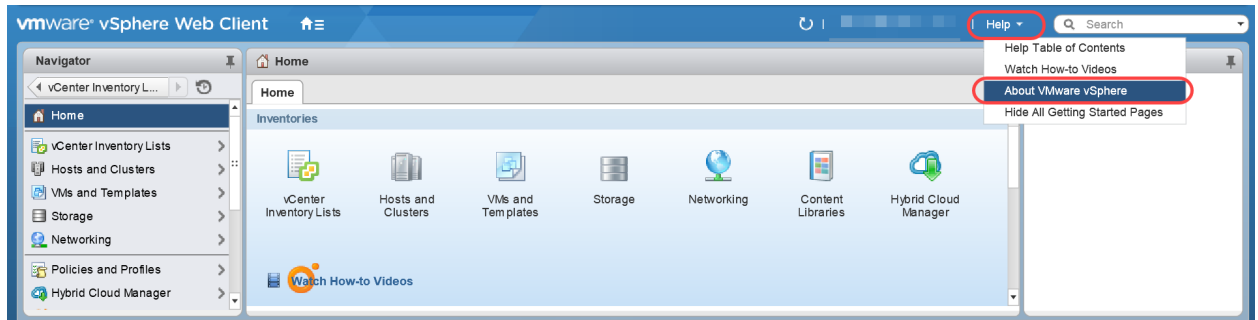
1. Review the VMware Version

Use the following instructions to confirm VMware vSphere vCenter has v7.0 or v8.0 installed.

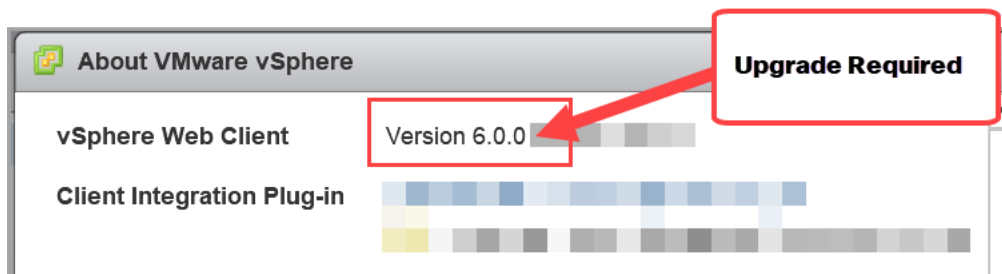


The menus and graphics in your VMware UI may vary from what you see here. Refer to your VMware guide for details specific to your environment.

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, v6.5, or v6.7, you need to upgrade it to v7.0 or v8.0. Refer to your VMware guide for instructions.



5. Continue to the next section.

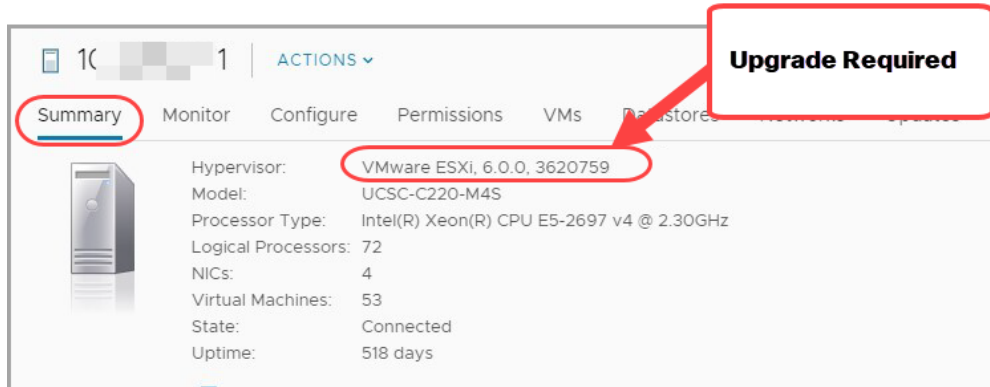
2. Review the VMware Hosts

Use the following instructions to review the ESXi host and confirm it has v7.0 or 8.0 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, v6.5, or v6.7, you need to upgrade it to v7.0 or 8.0. 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 rapid release 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 the [Virtual Edition Appliance Installation Guide](#); 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 the **Enable SSH** check box to enable SSH access on the appliance.
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.

Certificate Validity

Confirm your appliance identity certificates are valid and current before you start the update process. We cannot update appliances with invalid or expired appliance identity certificates. To replace an appliance identity certificate, follow the instructions in the [SSL/TLS Certificates for Managed Appliances Guide](#).

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

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.

- **Enabling SSH:** Follow the steps in [Alternative Access](#) to enable SSH on all Data Nodes and be sure to select the **Enable SSH** check box 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.
- **Update all Data Nodes v7.4.1 or later:** If you have v7.4.1 or later installed, follow the instructions to use the **Update all Data Nodes** button to update your Data Nodes at the same time. You will use the button for installing patches and the SWU file. You may need to start the Data Store Database after a patch install, but it will start automatically after an update SWU is successfully installed on all Data Nodes.
- **Downtime:** If you're concerned about the downtime required for this update, please contact [Cisco Support](#).

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 v7.5.0. 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 7.5.0](#) 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 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 Manager > **Client Group** column and check each Manager in the list. If Cisco Adaptive Network Control (ANC) is not shown, check the 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.

- **i** 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 7.5.0](#) 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.

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 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).
- **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 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 Manager, then select the **Global Settings** icon > **Central Management**. Click the **⋮ (Ellipsis)** icon in the **Actions** column 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 Manager, then select the **Global Settings** icon > **Central Management**. Click the **⋮ (Ellipsis)** icon in the **Actions** column 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 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 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 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.

MongoDB Upgrade

We will check your CPU configuration before the update. During the update, we will upgrade MongoDB to v6.0.9.

CPU Instruction Set Requirement: Ensure that your CPU is capable of the AVX/AVX2 instruction sets. For ESXi, select a VM hardware version of 11 or greater. For KVM, we recommended that you utilize host passthrough.

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.

Managers and Flow Collectors

- **Flow Collectors** After a Flow Collector is updated and running, it will cache data to be sent to the 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 Manager to lose all of the historical data for those Flow Collectors.

Communications

During the update process, communications will stop between the 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 completed, communications are re-established and the appliance status displays as **Connected**. See [9. Install the v7.5.0 Software Update](#) for more information.



Make sure the appliance status displays as **Connected** 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 Manager and Flow Collector**
- 6. Back Up Data Store**
- 7. Check the Available Disk Space**
- 8. Install Patches**
- 9. Install the v7.5.0 Software Update**
- 10. Configure High Availability**
- 11. Install the Desktop Client**
- 12. Verify 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 version **7.4.0**, **7.4.1**, or **7.4.2**, complete the following steps:

1. Log in to your Manager as admin using your Manager IP address.
Type `https://<Manager IP address>` in your browser address bar.
2. **7.4.0 and 7.4.1:** Click the (**Global Settings**) icon. Select **Central Management**.
7.4.2: Select **Configure > GLOBAL Central Management**.
3. Select the **Update Manager** tab, and locate the **System Updates** section.

Appliance Type	Host Name	IP Address	Last Reboot	Installed Version	Ready To Install	Update Status	Actions
Manager	10.255.255.9	10.255.255.9	3 hours ago	7.4.0 20210820.2004-7a3528073a67-0	-		...
Manager	10.255.255.10	10.255.255.10	4 hours ago	7.4.0 20210820.2004-7a3528073a67-0	-		...
Flow Collector	10.255.255.11	10.255.255.11	7 hours ago	7.4.0 20210820.2004-7a3528073a67-0	-		...
Flow Collector	10.255.255.12	10.255.255.12	7 hours ago	7.4.0 20210820.2004-7a3528073a67-0	-		...
UDP Director	10.255.255.13	10.255.255.13	7 hours ago	7.4.0 20210820.2004-7a3528073a67-0	-		...
Flow Sensor	10.255.255.14	10.255.255.14	3 hours ago	7.4.0 20210820.2004-7a3528073a67-0	-		...



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

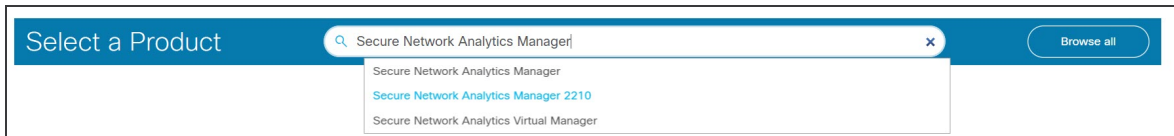
To manage your licenses, download patches, and download update files, log in to your Cisco Smart Account at <https://software.cisco.com>.

Use the following instructions to download patches and the v7.5.0 SWUs listed on your account.

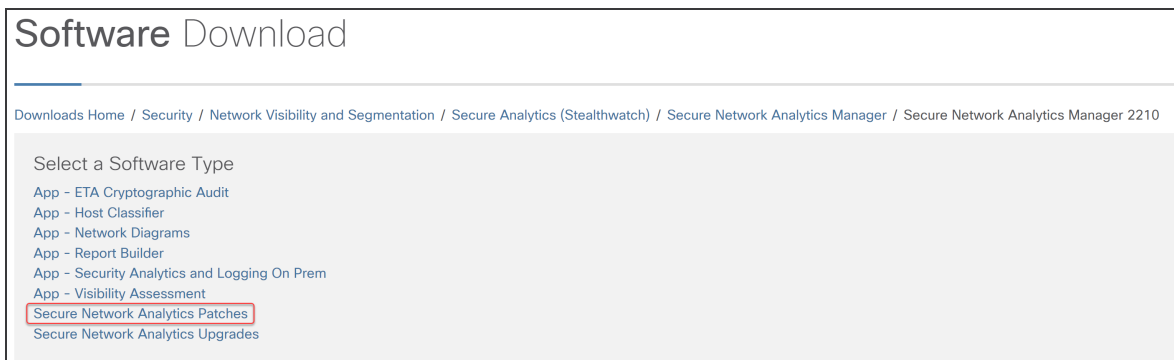
1. Log in to Cisco Software Central

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 **Secure Network Analytics Patches** to access any patch files you need to apply before beginning the update process



- or select **Secure Network Analytics 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
- Secure Network Analytics Patches
- Secure Network Analytics Upgrades

2. Download Patches

i Select **Secure Network Analytics 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 **Secure Network Analytics Patches**, the appliance page displays.

1. Select the version of Secure Network Analytics currently installed on your appliances. For example, if your appliances have 7.4.1 installed, select **7.4.1**.

Software Download

Downloads Home / Security / Network Visibility and Segmentation / Secure Analytics (Stealthwatch) / Secure Network Analytics Manager / Secure Network Analytics Manager 2210 / Secure Network Analytics Patches- 7.4.1

Search...

Expand All Collapse All

Latest Release

- 7.4.1
- Certificate Bundles
- 7.3.2
- 7.1.3

All Release

- Certificate Bundles
- Firmware

Secure Network Analytics Manager 2210

Release 7.4.1

My Notifications

Related Links and Documentation

- No related links or documentation -

File Information	Release Date	Size	
7.4.1-PATCH SMC Rollup #7 patch-smc-ROLLUP007-7.4.1-v2-01.swu	07-Feb-2023	4665.39 MB	Download

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 the patches for your current version, including the latest rollup patch for each of your appliances, and also the required common update patches, CIMC firmware update patches, and Cisco bundles patches.

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 Manager first.

After you select **Secure Network Analytics Upgrades**, the appliance page displays.

1. Select **7.5.0**.
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 of the required files for this update. If you are missing any files, see [2. Download the Patches and the Update Files](#) .

Appliance	Updating from v7.4.0, v7.4.1, or v7.4.2 Software Update File Name
UDP Director (also known as Flow Replicator) UDP Director VE (also known as Flow Replicator VE)	update-udpd-7.5.0.20231114.0021-18dba09f721e-0-v2-01.swu
Data Node	update-dnode-7.5.0.20231114.0021-18dba09f721e-0-v2-01.swu
Flow Collector database 5000 series	update-fcdb-7.5.0.20231114.0021-18dba09f721e-0-v2-01.swu
Flow Collector (NetFlow) (This is needed for the Flow Collector 5000 series engine) Flow Collector (NetFlow)VE	update-fcnf-7.5.0.20231114.0021-18dba09f721e-0-v2-01.swu
Flow Collector (sFlow) Flow Collector (sFlow) VE	update-fcsf-7.5.0.20231114.0021-18dba09f721e-D-v2-01.swu
Flow Sensor Flow Sensor VE	update-fsuf-7.5.0.20231114.0021-18dba09f721e-0-v2-01.swu
Manager Manager VE	update-smc-7.5.0.20231114.0021-18dba09f721e-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 Manager.
 - **All Managed Appliances:** To back up the configuration of all appliances managed by the Central Manager, select your primary 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**.

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



If you are backing up the 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 Manager and Flow Collector databases, see [5. Back Up Databases for the Manager and Flow Collector](#).

7. Continue to [4. Create a Diagnostics Pack](#)

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:

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`.

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.

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.

5. Back Up Databases for the Manager and Flow Collector



This procedure only applies to Non-Data Store Flow Collectors. Without a backup, you will not be able to recover your files if a problem occurs during the update process. Make sure you follow the instructions and complete all procedures for the database backup. For assistance, contact [Cisco Support](#).

After creating a diagnostics pack for the 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).

Database Storage Statistics

Capacity

	Average	Work
Capacity in Days	50	49
Remaining Days	22	21
Bytes Per Day	549.46M	563

Flow Data Summary

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

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.

Quick View for Flow

Exporter	Exporter Type	Interface	Direction	TTL	DSCP	Flow Action
	Cisco	#Index-2	Outbound			Permitted
	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 Manager and Flow Collector databases using the following instructions.



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

1. Log in to the 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;"
```

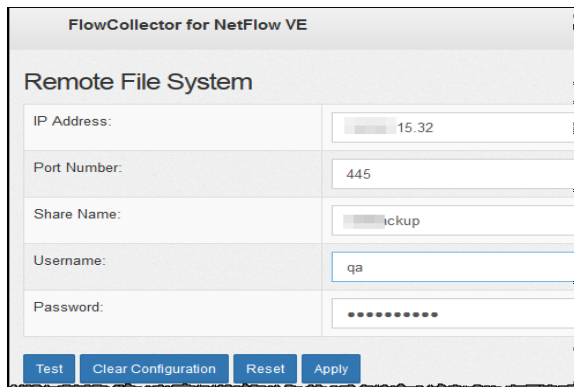

3. Back Up to Remote File System

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

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'. The page contains the following fields and values:

Field	Value
IP Address:	15.32
Port Number:	445
Share Name:	backup
Username:	qa
Password:

At the bottom of the form, there 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.

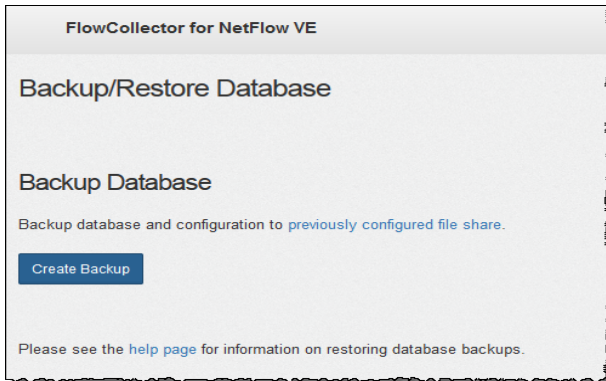
If the Apply button is not enabled after you enter the password, click once in a blank area on the Remote File System page to enable it.

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 Manager and Flow Collector databases.



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

1. Log in to the 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 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 [System Configuration Guide](#) for more information on Data Store database backup.

To backup your Data Store, complete the following procedures:

1. Estimate Backup Host Storage Requirements

2. Prepare a Backup Host with twice the storage capacity of the backup size. Install Python v3.7 and rsync v3.0.5 on the backup host.

i Use a Linux-based host separate from your Secure Network Analytics appliances.

3. Enable Passwordless SSH Access for dbadmin. Make sure all Data Nodes can reach the backup host using passwordless SSH access.

4. Initialize the Backup Directory on the Backup Host

5. Back Up the Data Store Database

1. Estimate Backup Host Storage Requirements

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

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

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

2. Prepare a Backup Host

1. Based on the storage requirements you estimated in **1. Estimate Backup Host 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 Secure Network Analytics appliances.

2. Log into the backup host console as `root`.
3. From the command prompt, enter `python3 --version` and press Enter to see what version of Python you have installed. You have the following options:
 - If Python 3.7 or later is installed, go to [step 6](#).
 - Otherwise, install Python 3.7, beginning with step 4.
4. Enter `sudo apt-get update` and press Enter to download updated versions of packages, including Python. Enter your password when prompted.
5. Enter `sudo apt-get install python3.7` and press Enter to install Python 3.7 (modify the command to install a different version).
6. From the command prompt, enter `rsync --version` and press Enter to see what version of rsync you have installed. You have the following options:
 - If rsync 3.0.5 or later is installed, continue to [step 9](#).
 - Otherwise, install rsync 3.0.5. Continue to step 7.
7. Enter `sudo apt-get update` and press Enter to download updated versions of packages, including rsync. Enter your password when prompted.
8. Enter `sudo apt-get install rsync` and press Enter to install rsync.
9. From the command prompt, enter `getent passwd | grep dbadmin` and press Enter to determine if a `dbadmin` user account exists on this host. You have the following options:
 - If a `dbadmin` user account exists, the backup host is ready. Continue to [3. Enable Passwordless SSH Access for dbadmin](#).
 - Otherwise, create a `dbadmin` user account on this host. Continue to step 10.
10. From the command prompt, enter `adduser dbadmin` and press Enter to create a `dbadmin` user account.
11. Enter `passwd dbadmin` and press Enter to assign a password to `dbadmin`.
12. Enter a **New password** and press Enter to set the `dbadmin` password. Confirm the password when prompted.

3. Enable Passwordless SSH Access for dbadmin

1. 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.
2. Review the OpenSSH documentation on `ssh-copy-id dbadmin@<hostname>` for more information.
3. Log into the first Data Node as `dbadmin` by typing the following:

```
su dbadmin
```

4. Copy the following command and paste it into a plaintext editor:

```
ssh-copy-id dbadmin@[hostname] where [hostname] is the backup host's hostname or IP address.
```


5. Copy the updated command, paste it into the command prompt, and press Enter to copy the `dbadmin` SSH authorized key to the backup host.
6. Copy the following command and paste it into a plaintext editor:

```
ssh 'dbadmin@[hostname]' where [hostname] is the backup host's hostname or IP address.
```

7. Copy the updated command, paste it into the command prompt, and press Enter to verify that you can log into the remote host's console over SSH without needing a password from this Data Node.

4. Initialize the Backup Directory on the Backup Host

1. Log in to the first Data Node console as `root`.

 Note the Data Node you use to initialize the backup directory. You will use the same Data Node to back up the Data Store database in a later procedure (**5. Back Up the Data Store Database**).

2. Enter `su - dbadmin` and press Enter to run the following commands as the `dbadmin` user.
3. Enter `ssh [backup-host]` where `[backup host]` is the hostname or ip address of your backup server. You should be able to 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.
4. Enter `cd /home/dbadmin` and press Enter to change directories.
5. Enter `mkdir backups` and press Enter to create the `backups` directory.
6. Enter `exit` and press Enter to return to the Data Node's command line prompt.

7. Enter `vi pw.ini` and press Enter to create the `pw.ini` backup password file, and edit it.

i If you updated 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.

8. Copy the following lines to a plaintext editor:

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

9. Update `[dbadmin-password]` to the Data Store `dbadmin` password.
10. Copy the updated lines and paste them into the `pw.ini` backup password file.
11. Press Esc, then enter `:wq`, then press Enter to exit and save your changes.
12. 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. If you are using v7.4.2 software, skip to [step 15](#). Otherwise, proceed to the next step.
13. For each node, edit/modify `SSHD_OPTS` in the `/etc/default/ssh` file as shown below. You will have to log in as `root` to complete this process.

Before:

```
SSHD_OPTS="-o AllowUsers=root -o AllowUsers=sysadmin -o
Banner=/etc/issue.net -o PermitRootLogin=yes -o
AllowTcpForwarding=no"
```

After:

```
SSHD_OPTS="-o AllowUsers=root -o AllowUsers=sysadmin -o
AllowUsers=dbadmin -o Banner=/etc/issue.net -o
PermitRootLogin=yes -o AllowTcpForwarding=yes"
```

14. Restart the `ssh` service as follows:

```
systemctl restart ssh
```

15. Copy the following lines and paste them into a plaintext 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

```

16. Enter `vi config.ini` and press Enter to create the `config.ini` backup configuration file and edit it.
17. Copy the text you pasted into a plaintext editor in step [15](#) and paste it into your `config.ini` file.
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 these host names. To determine your Data Node node names, do the following:
 - Connect to any Data Node console as `root`
 - Enter `su dbadmin`
 - Enter `admintools -t node_map`
 - Use the node names in the “NODENAME” column for the `[Mapping]` entries

Example:

```

dbadmin@sdbn-742-10-0-56-133-5:/root$ admintools -t node_map
DATABASE   | NODENAME                               | HOSTNAME
-----
sw         | v_sw_node0001                          | 169.254.42.10
sw         | v_sw_node0002                          | 169.254.42.12
sw         | v_sw_node0003                          | 169.254.42.15

```

20. Ensure that you have an entry for each Data Node if you deployed more than three to your environment. If you have only a single Data Node, remove the extra `[Mapping]` lines leaving only the one line for your single Data Node.
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.

5. Back Up the Data Store Database



You will only need to issue the backup command on one Data Node in order to back up your entire multi-node database.

1. As `root`, log into the console of the Data Node where you initialized the backup host directory in [4. 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. You have these options:
 - If the backup test resolves successfully, back up the Data Store and continue to step 4.
 - If the backup test fails, a snapshot file may have been created and must be removed. See [Data Store Backup Failure](#) for removal instructions. If the backup test fails to resolve, review the debug log files in the `/tmp/vbr` directory, resolve the root cause, then test the backup again. Contact [Cisco Support](#) for more assistance.
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](#).

Data Store Backup Failure

If your Data Store backup fails, make sure to remove the database snapshot before attempting another backup. Follow these steps to remove the Data Store database snapshot.

1. Connect to your Data Store database cluster using `vsq1`.
2. Execute the following command to retrieve a list of your snapshots:

```
select * from database_snapshots;
```

3. Replace 'snapshot_name' with the name of the snapshot that you want to remove, then execute the following command:

```
select remove_database_snapshot('snapshot_name');
```

4. Execute the following command to exit.

```
\q
```

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

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

Make sure you have enough available space on the 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 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 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 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).
- **Manager:** For example, if you upload four SWU files to the 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 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** (v7.4.0) or **Connected** (v7.4.1, v7.4.2) before you start the next patch installation.
- **Data Nodes (v7.4.1):** If you have Data Nodes with v7.4.1 installed, make sure to use the **Update All Data Nodes** button.

1. Review the Installed Version

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

1. Log in to your primary Manager.

Type `https://<Manager IP address>` in your browser address bar.

2. **7.4.0 and 7.4.1:** Click the  (**Global Settings**) icon. Select **Central Management**.
7.4.2: Select **Configure > GLOBAL Central Management**.
3. Review the **Appliance Status** column and confirm each appliance is shown as **Up** (v7.4.0) or **Connected** (v7.4.1, v7.4.2).
4. Select the **Update Manager** tab, and locate the **System Updates** section.

- Review the **Installed Version** column. Confirm each appliance is consistent, with only version **7.4.0**, **7.4.1**, or **v7.4.2** installed.

This example shows the Installed Version for all appliances is v7.4.0.

Appliance Type	Host Name	IP Address	Last Reboot	Installed Version	Ready To Install	Update Status	Actions
Manager	10.255.255.9	10.255.255.9	3 hours ago	7.4.0 20210820.2004-7a3528073a67-0	-		...
Manager	10.255.255.10	10.255.255.10	4 hours ago	7.4.0 20210820.2004-7a3528073a67-0	-		...
Flow Collector	10.255.255.11	10.255.255.11	7 hours ago	7.4.0 20210820.2004-7a3528073a67-0	-		...
Flow Collector	10.255.255.12	10.255.255.12	7 hours ago	7.4.0 20210820.2004-7a3528073a67-0	-		...
UDP Director	10.255.255.13	10.255.255.13	7 hours ago	7.4.0 20210820.2004-7a3528073a67-0	-		...
Flow Sensor	10.255.255.14	10.255.255.14	3 hours ago	7.4.0 20210820.2004-7a3528073a67-0	-		...

2. Install Required Patches

Make sure to install any required **v7.4.x** (v7.4.0, v7.4.1, or v7.4.2) patches before updating to v7.5.0.



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

On the **Update Manager** page:

- Click **Upload**.
- Select the latest rollup patch SWU file for the Manager.
- In the **Update Manager > System Updates** section, check the **Ready to Install** column for your Managers and confirm the patch is shown.
- Click the **Actions** menu for the secondary Manager, then choose **Install Update**.
 - Primary Manager:** If you've already finished the patch installation on the secondary Manager, click the **Actions** menu for the primary Manager.
 - Data Nodes v7.4.1 and later:** Click the **Update all Data Nodes** button.
 - All Other Appliances and Versions:** In the Actions column, click the **...** (Ellipsis) icon for the appliance. Select **Install Update**.
- 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** (v7.4.0) or **Connected** (v7.4.1, v7.4.2), review the **Central Management > Appliance Manager** page.

6. Confirm Installation:

- Click the **Actions** menu for the 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](#).
7. Review the Manager on the **Central Management > Appliance Manager** page. Confirm the appliance status is shown as **Up** (v7.4.0) or **Connected** (v7.4.1, v7.4.2).
 8. If you have two Managers configured for failover, repeat steps 4 through 7 to install the patch on the primary Manager.
 9. 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;"> <p> Prior to v7.4.1, your cluster will not have both Data Nodes and Flow Collector 5000 Series Database.</p> </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 or Connected before proceeding.</p> <p>Update all Data Nodes (v7.4.1 and later)</p> <p>If you have v7.4.1 or later installed, follow the instructions to use the Update all Data Nodes button to install the patch on your Data Nodes at the same time. Make sure you restart Vertica on any Data Node after the update patch is successfully installed on all Data Nodes.</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 or Connected before you start the engine update.</p>
3.	Flow Collector 5000 Series Engine	<p>Make sure the Flow Collector series database completes the patch installation and the appliance status is shown as Up or Connected before you start the engine update.</p>
4.	All Other Flow Collectors (NetFlow and sFlow)	<p>Make sure the Flow Collector completes the patch installation and the appliance status is shown as Up or Connected before you install the patch on the next appliance in your cluster.</p>
5.	Flow Sensors	

10. Confirm Installation:

- Click the **Actions** menu for the appliance.
- 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](#).

11. 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** (v7.4.0) or **Connected** (v7.4.1, v7.4.2), review the Central Management > Appliance Manager page.

12. **Data Nodes v7.4.x:** After the patch file is installed successfully on all Data Nodes, restart Vertica on any Data Node.

- Go to Central Management > Data Store > Database Control.
- Click the **⋮ (Ellipsis)** icon in the Actions column for the database.
- Choose **Start**.
- Confirm the database status is shown as **Up**.

9. Install the v7.5.0 Software Update

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

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.
- **Confirm:** Confirm the update is installed and that each appliance status displays as **Connected** before you begin the next appliance update.
- **Multiple Appliances:** With the exception of 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.
- **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** check box 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:

i Make sure to upload all SWU files before you begin installing any SWU files.


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 or Connected before you update the primary UDP Director.</p> <div style="border: 1px solid #00a0e3; padding: 5px;"> <p>When you are upgrading the primary UDP Director, the secondary UDP Director will show an appliance status of "Config Channel Down" until the upgrade of both the</p> <p>i primary and secondary UDP Director is complete. Once both appliances are upgraded and the automatic reboot occurs, the appliance status for both UDP Directors will change to "Connected."</p> </div>
2.	All Data Nodes or Flow Collector 5000 Series Database	<div style="border: 1px solid #00a0e3; padding: 5px;"> <p>i Prior to v7.4.1, 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.</p>

		<p>Refer to Data Store in the Introduction for more information.</p> <p>Update all Data Nodes (v7.4.1 and later)</p> <p>If you have v7.4.1 and later installed, follow the instructions to use the Update all Data Nodes button to update your Data Nodes at the same time. Make sure you restart Vertica on any Data Node after the update SWU file is successfully installed on all Data Nodes.</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 or Connected before you start the engine update.</p>
3.	Flow Collector 5000 Series Engine	Make sure the engine update is completed and the appliance status is shown as Up or Connected before you update the next appliance in your cluster.
4.	All Other Flow Collectors (NetFlow and sFlow)	Make sure the Flow Collector update is completed and the appliance status is shown as Up or Connected before you update the next appliance in your cluster.
5.	Flow Sensor(s)	Upload the Flow Sensor SWU file.
6.	Secondary Manager *if used	If your system uses a secondary Manager confirm the secondary Manager update is completed and

		<p>confirm the secondary Manager appliance status is shown as Up or Connected before you start the primary Manager update.</p> <p>After the update completes, both Managers may restart in the secondary role. If this occurs, refer to 12. Verify Manager Failover Roles for details. Do not change the failover roles until both Managers are updated.</p>
7.	Primary Manager	<p>If your system uses a secondary Manager, confirm the secondary Manager update is completed and confirm the secondary Manager appliance status is shown as Up or Connected before you start the primary Manager update.</p> <p>After the update completes, both Managers may restart in the secondary role. If this occurs, refer to 12. Verify Manager Failover Roles for details. Do not change the failover roles until both 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 7.5.0 SWUs

1. Log into your Manager:

Type `https://<Manager IP address>` in your browser address bar.

2. **7.4.0 and 7.4.1:** Click the  (**Global Settings**) icon. Select **Central Management**.
7.4.2: Select **Configure > GLOBAL Central Management**.
3. 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 displays as **Connected** before you start the next appliance update.

4. Review the **Installed Version** column. Confirm each appliance has the same version **7.4.0**, **7.4.1**, or **v7.4.2** installed.

This example shows that all appliances have the same installed version, 7.4.0. Note that all appliances have the same installed version.

System Updates							
Appliance Type	Host Name	IP Address	Last Reboot	Installed Version	Ready To Install	Update Status	Actions
Manager	10.255.255.9	10.255.255.9	3 hours ago	7.4.0 20210820.2004-7a3528073a67-0	-		...
Manager	10.255.255.10	10.255.255.10	4 hours ago	7.4.0 20210820.2004-7a3528073a67-0	-		...
Flow Collector	10.255.255.11	10.255.255.11	7 hours ago	7.4.0 20210820.2004-7a3528073a67-0	-		...
Flow Collector	10.255.255.12	10.255.255.12	7 hours ago	7.4.0 20210820.2004-7a3528073a67-0	-		...
UDP Director	10.255.255.13	10.255.255.13	7 hours ago	7.4.0 20210820.2004-7a3528073a67-0	-		...
Flow Sensor	10.255.255.14	10.255.255.14	3 hours ago	7.4.0 20210820.2004-7a3528073a67-0	-		...

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



Make sure to upload all SWU files before you begin installing any of the SWU files.

- **Updates:** Upload a SWU file for each appliance type in Central Management.
- **Disk Space:** See [7. Check the Available Disk Space](#) if you need to confirm you have enough disk space.

2. Install the 7.5.0 SWU

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



Make sure you update the appliances in order and review the note information. See [Update Order](#).

1. Confirm the appliance status for all appliances is shown as **Up** (v7.4.0) or **Connected** (v7.4.1, v7.4.2).
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 **7.5.0** SWU file is posted.
 - **Last Reboot of Managers and Flow Collectors:** .
 - 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** (v7.4.0) or **Connected** (v7.4.1, v7.4.2), review the **Central Management > Appliance Manager** page.

4. **Data Nodes v7.4.1 and later:** Click the **Update all Data Nodes** button.

All Other Appliances and Versions: In the Actions column, click the **⋮ (Ellipsis)** icon for the appliance. Select **Install Update**.

5. 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.

6. Check the **Installed Version** column to confirm it shows the version **7.5.0** software update.
 - **Installation Successful:** If **7.5.0** 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](#).
7. On the Security Insight Dashboard, choose **Configure > GLOBAL Central Management**, then locate the appliance in the inventory.
 - **Up or Connected:** Confirm the appliance status is shown as **Up** (v7.4.0) or **Connected** (v7.4.1, v7.4.2). After you install the primary Manager, the appliance status shows as **Connected** for all successfully installed appliances in v7.5.0.
 - **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**.
8. **Data Nodes v7.4.1 to v7.5.0:** Confirm the following status for all Data Nodes:
 - Go to the **Data Store > Database Update Status** tab. Confirm the Data Node Update Status for all Data Nodes is shown as **Succeeded** and the Last Status Change is current. You may need to refresh the page to see the most recent status.

- Click the **Database Control** tab. Confirm the Database Status is shown as **Up**. Confirm the status for all Data Nodes is shown as **Up**.
9. Repeat all steps in this section, **2. Install the 7.5.0 SWU**, for the next appliance. Make sure you update the appliances in order.
- If you've updated every appliance in Central Management to v7.5.0, 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	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 Managers.
Loss of network connectivity between the Manager and the managed appliances	Restore the network connectivity and confirm each appliance is shown as Up or Connected on the Appliance Inventory. If the appliance status is Config Channel Down , refer to the Troubleshooting section of the System Configuration Guide for instructions. Retry the patch or software update file installation after you confirm network connectivity is restored.
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.	Confirm that you have the correct SWU. If you're unable to determine whether you have the correct SWU, contact Cisco Support .
No space left on device (Disk Space)	Check the disk space on each appliance to confirm you have enough available space to install patches and software update files. On each managed appliance, you need at least 4 times the size of the individual software update file (SWU) available. On the Manager, you need at least 4 times the size of all appliance SWU files that you upload to Update Manager. <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).


Error Description or Category	Details
	<ul style="list-style-type: none"> • Manager: For example, if you upload four SWU files to the 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 or Connected on the Appliance Inventory. If the appliance status is Config Channel Down, refer to the Troubleshooting section of the System Configuration Guide for instructions.</p>
Upload Failed	<p>Confirm each upload is completed and shown in the Ready to Install column before you start uploading another SWU file. You can also review the log file:</p> <pre>/lancope/var/logs/containers/svc-central-management.log</pre> <p>to review why the upload failed.</p> <p>See 9. Install the v7.5.0 Software Update for more information. If you continue seeing this error message, contact Cisco Support.</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**.

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. Follow the on-screen prompts to open the Desktop Client and trust the appliance identity certificate.
8. Enter the Manager user name and password.

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. Follow the on-screen prompts to open the Desktop Client and trust the appliance identity certificate.
8. Enter the Manager user name and password.

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.

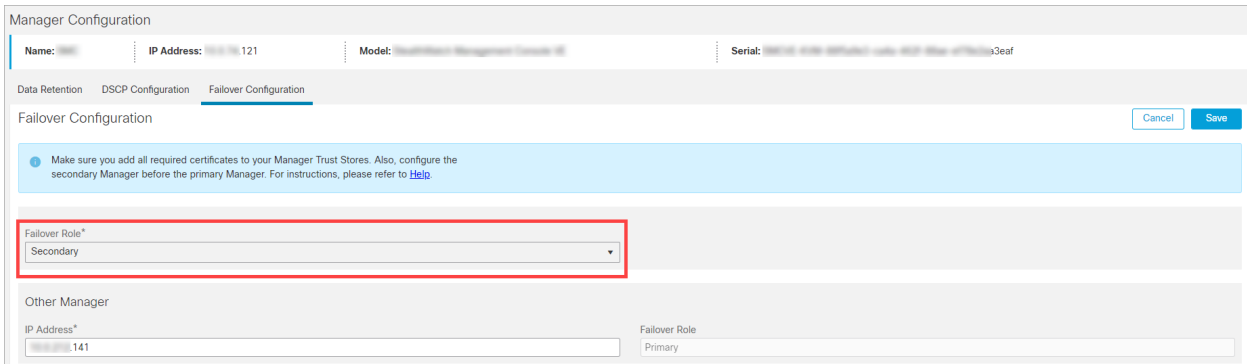
12. Verify Manager Failover Roles

 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 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. Select **Configure > GLOBAL Manager**.
3. Click the **Failover Configuration** tab.
4. Confirm the **Failover Role** is shown as **Secondary**.




Manager Configuration

Name: [redacted] IP Address: 141.121 Model: [redacted] Serial: [redacted]

Data Retention DSCP Configuration **Failover Configuration**

Failover Configuration Cancel Save

 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](#).

Failover Role*
Secondary

Other Manager

IP Address* 141 Failover Role Primary

5. Log in to the **primary** Manager. Follow steps 2 through 4 to confirm the **Failover Role** is shown as **Primary**.
6. 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](#).

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



9. **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.
- Select **Configure > GLOBAL Central Management**.
- Locate the Flow Collector in the inventory.
- 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.

10. Log in to the primary Manager.

11. Review the **Central Management Inventory**. 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>

Change History

Document Version	Published Date	Description
1_0	December 13, 2023	Initial Version.
1_1	July 12, 2024	Fixed an incorrect reference to v7.4.2.

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)

