Stealthwatch® System Version v6.9.x to v6.10.6 Update Guide

Use this guide to update the following Stealthwatch appliances from v6.9.x to v6.10.6:

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

For details on v6.10.6, refer to the Release Notes.

**Important:** If your appliances have version 6.10.1, 6.10.2, 6.10.3, 6.10.4, or 6.10.5 installed, use the Stealthwatch System Version 6.10.x to 6.10.6 Update Guide to update your appliances. Do not use this guide.

**CAUTION!**

- 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.
- Before you update your system, back up the configuration and create a diagnostics pack as described in this guide. We also strongly recommend backing up the database for Flow Collectors and the SMC. 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.
- The SMC and Flow Collector must have been running for **greater than one hour but less than seven days** before you begin the update process. If it has not, the SWU files will not install due to a migration safety switch.
- Make sure to update the appliances in this order: first, all UDP Directors/FlowReplicators (if any), Endpoint Concentrators, all of the Flow Collectors, followed by the secondary SMC (if used), then the primary SMC, finally all Flow Sensors (if any).

**Important:**

- If you have Stealthwatch System v6.5.x, you must update from v6.5.x to v6.6.x, from v6.6.x to v6.7.x, from v6.7.x to 6.8.x, v6.8.x to 6.9.x, and then from v6.9.x to v6.10.6. Each update guide is available on the Customer Community.
- Make sure you install the latest rollup patch before the upgrade. Go to the Stealthwatch Download and License Center at [https://stealthwatch.flexnetoperations.com](https://stealthwatch.flexnetoperations.com).
Due to an error with the system upgrade file, upmanrepo.swu, you will have to use the individual appliance swu files to update your system.

- If FIPS mode was enabled in an earlier software version (prior to v6.10.6), disable FIPS mode before you update the software to v6.10.6. See Disabling FIPS Mode for details.
- When the update process is finished, the appliance automatically restarts. It does not collect new data during the restart process. However, your current data is preserved.
- For increased security, we recommend updating the IDentity 1000/1100 appliance to v3.3.0.x to take advantage of the new OpenSSL version with TLS 1.2.
- Check your Stealthwatch appliance’s NTP settings and remove the 130.126.24.53 NTP server if it is in the list of servers. This server is known to be problematic and it is no longer in Cisco’s default list of NTP servers to use.

Notes:
- This document uses the term "appliance" for any Stealthwatch product, including virtual editions (VEs) such as the Flow Collector VE.
- Stealthwatch does not support installing 3rd party applications on appliances.
- Stealthwatch requires Java version 8 (latest available update) to run the Stealthwatch Desktop Client. We do not support Java versions 9, 10, or 11. When you update your SMC to Stealthwatch v6.10.6, Oracle Java will no longer be used to install and open the Stealthwatch Desktop Client. To install the Stealthwatch Desktop Client after the v6.10.6 update, refer to the Stealthwatch Release Notes v6.10.6.
- Stealthwatch requires TLS v1.1 or later.
- Stealthwatch supports the latest version of Chrome, Firefox, Edge, and Internet Explorer v11.
- There may be a file size limitation with Microsoft Edge. We do not recommend using Microsoft Edge to upload the software update files (SWU).
- Where once the setting "disabled" for a security event disabled the event, now disabling will disable the alarm.
- To view the supported hardware platforms for each system version, refer to the Hardware and Version Support Matrix.

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

The images used in this guide are mostly of the Flow Collector NetFlow VE Admin interface, but it serves only as an example for all the appliances. The procedure for updating appliances is the same except where noted.

Before You Begin: Make Sure You Are Ready to Update

Before you begin the update process, consider the following items.

Best Time to Update

The update process generally takes approximately 30 minutes to complete per appliance. This estimate does not include the time needed to create backups and diagnostic packs, which can vary depending on your environment.

We recommend that you update the entire system at one time when your system will be experiencing relatively low volumes of traffic. After a Flow Collector is updated and running, it will cache data to be sent to the SMC until the SMC is updated. However, you will not want that process to run for a long time. Preparing all appliances so they can be updated at once is the most successful approach.

CAUTION! Do not delete any Flow Collectors from the SMC client interface. Doing so will cause the SMC to lose all of the historical data for those Flow Collectors.

Communications

During the update process, communications will stop between the SMC and the Flow Collectors. When this happens, the Flow Collector icons on the Enterprise tree in the SMC client interface will display a red “x” and the managed appliance icon will be orange (📸) instead of green.

In addition, if you have any Stealthwatch Flow Sensors, you will see a Flow Sensor Management Channel Down alarm on the Alarm Table in the SMC client interface. When the update is complete, communications are re-established, the icons return to normal appearance, and the alarm disappears.
Browser Shortcuts

If you use browser shortcuts to access the Appliance Admin interface for any of your Stealthwatch appliances, the shortcuts may not work after the update process is complete. In this case, simply delete the shortcuts and recreate them.
Alternative Access

WARNING!

It is important to enable an alternative method to access your Stealthwatch appliances for any future service needs, using one of the following:

**Hardware**


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


**Virtual Machines**

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

*If you cannot log in to the appliance using these methods*, you can enable SSH on the appliance network interface temporarily.

**WARNING!** When SSH is enabled, the system’s risk of compromise increases. It is important to enable SSH only when you need it. When you are finished using SSH, disable it.

1. Log in to the Appliance Admin interface.
   - SMC: Log in to the SMC. Click the **Settings** icon > **Administer Appliance**.
2. Click **Configuration** > **Services**.
3. Check the **Enable SSH** check box to enable SSH.
To allow the root user SSH access, check the **Enable Root SSH Access** check box.

4. Click **Apply**.

## UPDATE PROCESS

**CAUTION!** When performing an update, you must update your entire system in the order described in this guide. Otherwise, your system may be left in an unknown state.

**Important:** If your system uses a secondary SMC, update the secondary SMC before you update the primary SMC. After the update completes, both SMCs may restart in the secondary role. If this occurs, log in to the SMC client interface as the admin user and reset the primary SMC to the Primary Failover Role. Do not change the Failover Roles until both SMCs are updated.

**Note:**
- If you have only Flow Sensors, you can use these instructions to update only your Flow Sensors.
- The Flow Collector 5000 series Database should be updated before the Flow Collector 5000 series Engine. All Flow Collectors must be updated before updating any SMCs.

To ensure a successful update and minimize data loss, perform all of the procedures in this guide in this order.

1. Verify that the current version of the Stealthwatch appliance is 6.9.x.
2. Obtain the update files for the Stealthwatch appliances you need to update.
3. Disable FIPS Mode.
4. Back up the appliance configuration.
5. Create a diagnostics pack for the appliance
6. Back up the appliance database (for Flow Collectors and SMCs) and review available disk space.
7. Restart the appliance to ensure that all processes are in an organized state and wait at least one hour.
8. Update the appliances. Use the system update file first.
9. Verify the update.
10. Repeat these steps for the next appliance in the system. For best results, perform these procedures on each appliance in the following order:
    - All UDP Directors (also known as FlowReplicators)
    - Endpoint Concentrators
    - All NetFlow and sFlow Flow Collectors (update the Flow Collector 5000 series Database before the Engine)
    - Secondary SMC (if used)
VERIFYING THE CURRENT VERSION OF THE APPLIANCE

Go to the System Management page in the SMC Web application interface to verify the current version of your appliances. For the other appliances not on the System Management page you need to go the Appliance Administration interface as you have done before to verify the current version.

Complete these steps to verify that the current software version for each appliance you will be updating is 6.9.x.

1. Go to your SMC dashboard page.
2. Click the Settings icon, and then select System Management.
   The System Management page opens.

3. Are you updating a Flow Collector 5000 series or an Endpoint Concentrator?
   ○ If yes, go to the next step.
   ○ If no, go to “Obtaining the Update Files,” the next section in this guide.

4. For a Flow Collector 5000 series or an Endpoint Concentrator, go to its Appliance Admin interface login page (https://[IP address]). The current software version appears under the appliance name.

5. Is the current version 6.9.x?
   ○ If yes, check that all of the other appliances are same version with the latest patch rollup. When finished, go to the next step.
   ○ If no, you need to update previous versions first by following this order. To update to 6.10.6, the appliances must be v6.9.x.

6. Go to “Obtaining the Update Files,” next in this guide.
**OBTAINING THE UPDATE FILES**

After verifying that the current software version of the appliances you want to update is v6.9.x, complete these steps to obtain the software update (SWU) files.

1. Go to [https://stealthwatch.flexnetoperations.com](https://stealthwatch.flexnetoperations.com). The Download and License Center Login page opens.

   ![Download and License Center](image)

   **Note:** To define your password for the first time, or if you have forgotten your login ID or password, click the Password Finder link and follow the onscreen instructions.

2. Enter your Login ID and Password in the appropriate fields, and then click **Login**. The Product Home page opens.

3. Under the Software Updates section, click the appropriate Stealthwatch Release link. The Product Search page opens with a list of all possible downloads associated with the selected release.

4. Locate the appropriate update (SWU) file as indicated in the following table and click **Download**.

**Notes:**

- Each type of appliance has only one unified update file for both the “virtual” (VE) and the “physical” appliance.
- You do not have to download separate appliance update files except for the Flow Collector 5000 series engine and database and the Endpoint Concentrator (the UDP Director/FlowReplicator also if it is not managed by the SMC).
- Check the file size of the SWU files. You will use them to confirm that there is enough disk space on the appliance for the update.
**Important:** For those systems that have many Stealthwatch System appliances, we recommend that you download and install a **system update file**, not individual appliance update files. The system update file includes updates for the SMC, Flow Collector, Flow Sensor, and UDP Director (also known as FlowReplicator). However, you still need to download and install individual appliance update files for the Flow Collector 5000 series (both engine and database) and the Endpoint Concentrator on the Update page of the corresponding Appliance Admin interface.

<table>
<thead>
<tr>
<th>Appliance</th>
<th>Update File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>System update file (for SMC, Flow Collector, Flow Sensor, and UDP Director/Flow Replicator)</td>
<td>system-upmanrepo-6.10.6-RC3-01.swu</td>
</tr>
<tr>
<td>Flow Collector for NetFlow (This is needed for the Flow Collector 5000 series engine)</td>
<td>update-fcnf-6.10.6.2019.07.24.1617-01.swu</td>
</tr>
<tr>
<td>Flow Collector for NetFlow VE</td>
<td></td>
</tr>
<tr>
<td>Flow Collector for sFlow VE</td>
<td></td>
</tr>
<tr>
<td>SMC and SMC VE</td>
<td>update-smc-6.10.6.2019.07.24.1618-01.swu</td>
</tr>
<tr>
<td>Flow Sensor Appliance</td>
<td></td>
</tr>
<tr>
<td>UDP Director (also known as FlowReplicator)</td>
<td>update-udp-6.10.6.2019.07.24.1612-01.swu</td>
</tr>
<tr>
<td>UDP Director VE (also known as FlowReplicator VE)</td>
<td></td>
</tr>
<tr>
<td>Endpoint Concentrator</td>
<td>update-ec-6.10.6.2019.07.24.1613-01.swu</td>
</tr>
</tbody>
</table>

The Export Compliance page opens.
5. Click **I Agree**. (If any other compliance pages or license agreements open, agree to them as well.) The Product Download page opens for the file you selected.

6. Click **FTP Download**. A dialog opens giving you the option to save the SWU file.
7. Save the file to your preferred location.
8. Do you need to download another update file?
   - If yes, in the left navigation pane, click **Product Home** and repeat steps 3 through 7.
   - If no, at the bottom of the left navigation pane, click **Logout**.

### Disabling FIPS Mode

If FIPS mode is currently enabled on the appliance (using an earlier version of software prior to v6.10.6), you must disable FIPS mode before you update the software to v6.10.6.

If FIPS mode is not enabled on the appliance, go to Back Up the Appliance Configuration.
To disable FIPS mode, complete the following steps:

1. Log in to the Appliance Admin interface as the admin user. The Home page opens.
2. Click Configuration > Global Settings.
3. Click the Enable FIPS check box to clear it.
4. Click Apply.
5. Follow the on-screen prompts to confirm your changes. The appliance reboots.

**BACKING UP THE APPLIANCE CONFIGURATION**

Complete these steps to back up its configuration.

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

1. Log in to the Appliance Admin interface as the admin user. The Home page opens.
2. Look at the IP address and host name shown on the Home page. Verify that this is indeed the appliance you want to update.
3. Click Support > Backup/Restore Configuration. The Backup/Restore page opens as shown in the example at right.
4. Under the Backup section, click Create Backup. A progress window opens and indicates when the process is finished as shown in the example below.

5. Click Download and save the backup (TGZ) file to your preferred location.
6. Click Close to close the progress window.
7. Go to “Creating a Diagnostics Pack,” next in this guide.
CREATE A DIAGNOSTICS PACK

After backing up the appliance configuration, complete these steps to create a diagnostics pack for the appliance you are updating. Having a diagnostics pack can be invaluable if you need to troubleshoot.

Important: 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.

1. Click Support > Diagnostics Pack. The Diagnostics Pack page opens as shown in the example below.

2. Click Create Diagnostics Pack. A progress window opens and indicates when the process is finished.

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

4. Click Close to close the progress window.

5. Are you updating either a Flow Collector or SMC?
   - If yes, go to “Backing Up a Flow Collector or SMC Database,” next in this guide.
   - If no, go to “Updating a Stealthwatch Appliance”
BACKING UP A FLOW COLLECTOR OR SMC DATABASE

After creating a diagnostics pack for a Flow Collector or SMC, you must back up the Flow Collector and SMC databases. This process involves completing the following procedures:

1. Disabling SNMP Polling for an SMC.
2. Backing Up the Databases.
3. Re-enabling SNMP Polling in the SMC.

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

Disabling SNMP Polling for an SMC

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

To disable SNMP polling, complete the following steps.

1. Launch the SMC client interface as the admin user (but do not close the Appliance Admin interface).
2. In the Enterprise tree, right-click an exporter and select Configuration > Exporter SNMP Configuration. The Exporter SNMP Configuration page for that domain opens as shown in the example at right.
3. Note the entry in the Default field. You will need to re-enter this information after you back up the databases.
4. From the Default drop-down list, select None. SNMP polling for this domain is now off.
5. Click OK.
6. Repeat steps 2–5 for each domain on your system.

Backing Up the Databases

To back up a Flow Collector or SMC database to a remote file system, complete the following steps.
Important: The remote file system must have enough space to store the database backup. This process backs up approximately 0.5 GB to 2 GB of data per minute. 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.

1. Before you get started, we recommend trimming the Flow Collector database. This will free up the available disk space for storing flows and reduce the amount of time it takes to back up the database. Refer to the instructions posted to the Customer Community.

2. Return to the Appliance Admin interface (but do not close the SMC client interface.)

3. Determine how much space you will need on the remote file system to store the database backup as follows:

   a. Click Home. The Home page opens.
   b. Scroll down to the Disk Usage section as shown in the example.
   c. Look at the Used (byte) column for the /nocope/var file system as shown in the example at right. You will need at least this much space plus 15% more on the remote file system to store the database backup.

   Important: You should also confirm that you have at least 3 times the size of the software update file (SWU) free on the /nocope/var/ partition, which is in the Available (byte) column. For example, if the software update file (from the Download and License Center) is 6 GB, you should have 18 GB available on the partition. When this is uploaded to the SMC, it will begin extracting the SWU's for the types of devices that it can update. During this extraction, additional gigabytes of space will be needed. Once the extraction is complete, the System SWU will be removed from the file system. If you need to expand the appliance disk space, see the Data Storage section of the Stealthwatch Management Console VE and Flow Collector VE Installation and Configuration Guide.

4. Click Configuration > Remote File System. The Remote File System page opens as shown in the example below.
5. Complete the fields using the settings for the remote file system where you want to store the backup files.

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

6. When finished, click **Apply** to place the settings in the configuration file.

**Note:** 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.

   The message “Applying changes…” briefly appears as the settings are applied.

7. Click **Test** to verify that the Stealthwatch appliance and the remote file system can communicate with each other. You should see the following message at the bottom of the Remote File System page when the test is complete.

   **File sharing appears to be properly configured.**

8. Click **Support > Backup/Restore Database**. The Backup Database page opens as shown in the following example.
9. Click **Create Backup**. A progress window opens and indicates the status. Depending on the size of your database, and how often you perform a backup, this process may take a long time. When the backup process finishes, another progress window opens as shown in the example below, indicating that the backup process has completed.

![Backup Status - Started Thu Jan 26 2017 11:43:12 GMT-0500 (Eastern Standard Time)](image)

**Important:** 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.

10. If desired, click **View Log** to view details of the backup process.

11. Click **Close** to close the progress window. The Backup Database page updates, indicating that the backup completed and the length of time it took to complete the process.

---

**Re-enabling SNMP Polling in the SMC**

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

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

---

**RESTARTING THE STEALTHWATCH APPLIANCE**

Complete these steps to restart the Stealthwatch appliance you want to update. Restarting performs a disk check and helps to ensure that all processes are in an organized state before you begin the update. **This applies to all appliances to be updated.**
Important: The appliance does not collect data during the restart process. Depending on how long the appliance has been running, restarting can take only a few minutes or as long as 45 minutes to complete.

Note: For the SMC, click the Admin User drop-down list, and select Administer Appliance. Then log in as the admin user to the Appliance Admin interface.

1. Log in as the admin user to the Appliance Admin interface for the appliance you are updating. The Home page opens as shown in the example at right.
2. Click Operations > Restart Appliance. A confirmation window opens as shown in the example below.
3. Click Yes. A progress window opens and the appliance begins the restart process. Depending on how long the appliance has been running, restarting can take only a few minutes or as long as 45 minutes to complete. When finished, the Appliance Admin interface Login page opens.
4. Go to “Updating a Stealthwatch Appliance,” next in this guide.

UPDATING A STEALTHWATCH APPLIANCE

After creating a diagnostics pack (and backing up the database for a Flow Collector or SMC), complete these steps to update the Stealthwatch appliance.

There are two methods to update an appliance which depends on the type of appliance you are updating. You can start with the System Management page with either method but with the second method you must go to the Appliance Admin page.
1. For appliances included in the system update file (SMCs, Flow Collectors—excluding the Flow Collector 5000 series engine or database—UDP Directors (also known as FlowReplicators), and Flow Sensors) use the System Management page. Go to the next section, Updating a Stealthwatch Appliance through the System Management Page

2. For all other appliances, you must go to the corresponding Appliance Admin interface.

**Important:**
- The SMC and Flow Collector must have been running for **greater than one hour but less than seven days** before you begin the update process described in this section. If it has not, the SWU files will not install due to a migration safety switch. The SWU files have a safety check that allows the update process to run only during a certain time period after your system is rebooted and you reach this stage in the process. If it has taken more than six days to reach this stage in the upgrade process, you must reboot your system again and wait for one hour before you begin the update process described in this section.
- After the update process finishes, the Stealthwatch appliance restarts automatically. The appliance does not collect data during the restart process, which should take no more than 10 minutes to complete.

**Updating a Stealthwatch Appliance through the System Management Page**

You can use the System Management page to install updates of all appliances shown on the page.

**Important:**
- If your UDP Directors (also known as FlowReplicators) are configured as a High Availability (HA) cluster, update the secondary UDP Director first. Confirm the update is completed and the secondary UDP Director is running again before you update the primary UDP Director.
- If your system uses a secondary SMC, update the secondary SMC before you update the primary SMC.

1. If necessary, log in again to the SMC and click **Admin > System Management** to open the System Management page.

![](system_management_page.png)

2. Click the **Begin Upgrade** button to select the aggregated system update file (SWU) that you downloaded from the Download and License Center and upload it to the SMC. This system update file uploads the new
version for SMCs, Flow Collector, Flow Sensors, and UDP Directors (also known as FlowReplicators). (The file does not include the Flow Collector 5000 series engine or database.)

3. Click **Continue**. The Upload progress window opens.
4. Once the System SWU has been uploaded, click the **Actions** drop-down list for an individual appliance, and then click **Install Update** to update that appliance.

![Actions menu](image)

**Notes:** Remember to update in the following order:
1. UDP Director (also known as FlowReplicator)
2. Endpoint concentrator
3. All NetFlow and sFlow Flow Collectors
4. Secondary SMC
5. Primary SMC
6. All Flow Sensors

5. Click **Yes** on the Upgrade window.

   The Update Status cell will show that the appliance is being updated and will show Success or Failure with the reason for it after the update is complete.

6. Repeat steps 2 through 5 for all appliances shown the System Management page.
7. Do you have other appliances not listed on the System Management page?
   - If yes, go to **Updating a Stealthwatch Appliance through the Appliance Admin Interface**.
   - If no, go to the next step.
8. Continue to the next section to update the other appliances in your system.

### Updating a Stealthwatch Appliance through the Appliance Admin Interface

For each appliance not listed on the System Management page, complete the following steps:
1. Log in to the Appliance Admin interface.

2. Click **Support > Update**. If previous updates were applied, you will see them listed and can click the View Log link to see more details about them.

3. In the Upload Update File section, click **Browse**.

   **Note:** Be sure to select the appliance update files, not the system update file.

4. Navigate to select and open the update (SWU) file you downloaded earlier and saved. The file name appears in the Upload Update File field and the Upload button becomes active.

5. Do you want the update process to begin automatically as soon as you click **Upload**?
   - If yes, select the **Automatically Execute** checkbox.
   - If no (i.e., you want to launch the update process later), do not select the Automatically Execute checkbox, leaving it blank.

6. Click **Upload**. A confirmation window opens displaying the file name you selected.

7. Is the confirmation window displaying the correct update (SWU) file name?
   - If yes, click **OK**, then go to step 8.
   - If no, click **Cancel** to close the confirmation window. Go back to step 2.

8. Did you select the Automatically Execute checkbox?
   - If yes, a progress window opens showing first the upload status, and then the update status. Go to step 12.
   - If no, a progress window opens showing the upload status. Depending on the SWU file, the upload process can take up to five minutes to complete. When the upload process is finished, click **Close** to close the progress window. Note that the Execute Update File section now appears on the Update page. Go to step 9.

9. When you are ready to launch the update process, select the drop-down box in the Execute Update File section of the Update page and select the correct update file.
10. Click **Apply**. A confirmation window opens, displaying the file name you selected, as shown in the example at right.

11. Is the confirmation window displaying the correct update (SWU) file name?
   - If yes, click **OK**. A progress window opens showing the update status. Go to the next step.
   - If no, click **Cancel** to close the confirmation window. Go back to step 2.

12. Depending on the SWU file and the appliance, the update process can take up to 30 minutes to complete. When the update process is finished, the appliance automatically restarts. When the restart process is complete, you will see a session timeout message as shown in the example at right.

13. Click **OK**. The Appliance Admin interface Login window opens and displays the new software version as shown in the following example.

14. Go to the next section, “Verifying the Update.”

### Verifying the Update

After the appliance restarts and the Appliance Admin interface Login window opens, complete these steps to verify that the update completed correctly.

1. Log in as the admin user. The Update page opens.
2. Verify that the Last Update Status section shows that the update completed and was applied as shown in the example below. If desired, you can read details of the update process by clicking the View Log link.

![Last Update Status](image)

3. Click Home. The Home page opens.

4. Verify that the Version field shows the new software version as shown in the following example.

![System](image)

5. Do you have other appliances to update?
   - If yes, return to the “See "Stealthwatch® System Version v6.9.x to v6.10.6 Update Guide "” section of this guide, and repeat all of the procedures as directed for the next appliance.
   - If no, go to step 6.

6. Click Logout and close your browser.

7. Was the SMC you updated the primary SMC in a failover pair?

   ![Important](image)

   **Important:** Do not change the Failover Roles until both SMCs are updated.

   - If yes, it is possible the SMC restarted in the Secondary Failover Role, even though it was using the Primary Failover Role before the update. Essentially, you will have two secondary SMCs. If this occurs, go to the SMC client interface, log in as the admin user and reconfigure the two SMCs to the desired failover roles. For assistance, refer to the SMC Client Online Help.
   - If no, you have finished verifying the update.

Congratulations! You are finished updating your system.
CONTACTING SUPPORT

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

- Contact your local Cisco Partner
- Contact Cisco Stealthwatch Support
  - To open a case by email: [tac@cisco.com](mailto:tac@cisco.com)
  - For phone support: 1-800-553-2447 (U.S.)