# Table of Contents

**Introduction** ................................................................. 6  
Overview ................................................................................. 6  
Audience ............................................................................... 6  
Terminology ............................................................................ 6  
Abbreviations ........................................................................ 6  

**Before You Begin** ............................................................. 8  
Installation Requirements ...................................................... 8  
    Hardware ........................................................................ 8  
    Virtual Edition (VE) Appliances ....................................... 8  
Configuration Details ............................................................ 9  
Downloading Software ......................................................... 9  
Licensing ............................................................................... 9  
TLS ..................................................................................... 9  
Third Party Applications ....................................................... 9  
Browsers .............................................................................. 9  
Host Name ........................................................................... 10  
Domain Name ....................................................................... 10  
NTP Server .......................................................................... 10  
Time Zone ............................................................................. 10  

1. **Configuring Stealthwatch** .............................................. 11  
Preparation ........................................................................... 11  
Stealthwatch with a Data Store ............................................. 11  
Appliance Setup Tool Requirements ..................................... 11  
Managed .............................................................................. 11  
SMC Failover ......................................................................... 12  
Best Practices ....................................................................... 12  
Appliance Configuration Order ............................................. 13  
1. Log In .............................................................................. 15
2. Configure the Appliance ........................................................................................................... 16
3. Register the Stealthwatch Management Console ................................................................. 20
4. Add Appliances to Central Management .................................................................................. 21
5. Confirm Appliance Status ......................................................................................................... 23

2. Finishing Appliance Configurations .......................................................................................... 25
   UDP Director ............................................................................................................................... 27
   Configuring Forwarding Rules ................................................................................................. 27
   Configuring High Availability .................................................................................................. 28
      Primary Node and Secondary Node Requirements ............................................................... 29
   1. Configure the Primary UDP Director HA .......................................................................... 29
   2. Configure the Secondary UDP Director HA ....................................................................... 31
   Flow Sensor ................................................................................................................................. 32
      1. Configure the Application ID and Payload .................................................................. 32
      2. Configure the Flow Sensor to Identify Applications (optional) .................................... 35
      3. Restart the Appliance ................................................................................................. 36

3. Installing the Stealthwatch Desktop Client ............................................................................. 37
   Install the Desktop Client Using Windows .............................................................................. 37
   Change the Memory Size ......................................................................................................... 38
   Install the Desktop Client Using macOS ................................................................................ 39
   Change the Memory Size ......................................................................................................... 40

4. Verifying Communications ..................................................................................................... 41
   Verify NetFlow Data Collection ............................................................................................ 41

5. Licensing .................................................................................................................................. 44
   Evaluation Mode ....................................................................................................................... 44

Defining an SMC Failover Relationship ...................................................................................... 45
   Configuring Failover .................................................................................................................. 45
   Primary and Secondary Roles ................................................................................................. 45

Enabling the Threat Intelligence Feed ........................................................................................ 47
   License ......................................................................................................................................... 47
## Troubleshooting

- Config Channel Down .......................................................... 64
- Opening Appliance Administration Interface .......................... 64
- Replacing the Appliance Identity .......................................... 65
- Changing the Host Name, Domain Name, or IP Address .......... 65
- Opening the Appliance Setup Tool ....................................... 65
- System Configuration Overview ............................................ 66
- Changing the Trusted Hosts ................................................... 66
- Resetting Factory Defaults ................................................... 67
  - RFD of a Flow Collector (Special Instructions) ...................... 68
- Enabling/Disabling Admin Users .......................................... 68
- Enabling or Disabling Password Reset .................................. 68
- Resetting Passwords to Default Settings ............................. 69
  - Resetting the Admin Password on the SMC ....................... 69
  - Resetting Admin, Root, Sysadmin Passwords to Default ....... 69
- Changing Passwords ............................................................ 71
  - Changing the Sysadmin Password ..................................... 72
  - Changing the Root Password ............................................. 72
  - Changing the Admin Password on the SMC ....................... 72
  - Changing the Admin Password on All Other Appliances ....... 72

## Installing Patches and Updating Software

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

Overview
Use this guide to configure the following Cisco Stealthwatch® Enterprise hardware and Virtual Edition (VE) appliances to one managed system in v7.3.2:

- Stealthwatch Management Console (SMC)
- Stealthwatch Flow Collector
- Stealthwatch Data Node
- Stealthwatch Flow Sensor
- Stealthwatch UDP Director

For more information about Stealthwatch, refer to the following online resources:

- **Overview:**
- **Appliances:**

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

If you are configuring virtual appliances, we assume you have basic familiarity with VMware or KVM.

If you prefer to work with a professional installer, please contact your local Cisco Partner or Cisco Stealthwatch Support.

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

A "cluster" is your group of Stealthwatch appliances that are managed by the Stealthwatch Management Management Console (SMC).

Abbreviations
The following abbreviations may appear in this guide:
## Abbreviations

<table>
<thead>
<tr>
<th>Abbreviations</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS</td>
<td>Domain Name System (Service or Server)</td>
</tr>
<tr>
<td>dvPort</td>
<td>Distributed Virtual Port</td>
</tr>
<tr>
<td>ESX</td>
<td>Enterprise Server X</td>
</tr>
<tr>
<td>GB</td>
<td>Gigabyte</td>
</tr>
<tr>
<td>IDS</td>
<td>Intrusion Detection System</td>
</tr>
<tr>
<td>IPS</td>
<td>Intrusion Prevention System</td>
</tr>
<tr>
<td>ISO</td>
<td>International Standards Organization</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>KVM</td>
<td>Kernel-based Virtual Machine</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum Transmission Unit</td>
</tr>
<tr>
<td>NTP</td>
<td>Network Time Protocol</td>
</tr>
<tr>
<td>OVF</td>
<td>Open Virtualization Format</td>
</tr>
<tr>
<td>SMC</td>
<td>Stealthwatch Management Console</td>
</tr>
<tr>
<td>TB</td>
<td>Terabyte</td>
</tr>
<tr>
<td>UUID</td>
<td>Universally Unique Identifier</td>
</tr>
<tr>
<td>VDS</td>
<td>vNetwork Distributed Switch</td>
</tr>
<tr>
<td>VE</td>
<td>Virtual Edition</td>
</tr>
<tr>
<td>VLAN</td>
<td>Virtual Local Area Network</td>
</tr>
<tr>
<td>VM</td>
<td>Virtual Machine</td>
</tr>
</tbody>
</table>
Before You Begin

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

Installation Requirements

Before you configure Stealthwatch using this guide, install your hardware and virtual appliances using the following guides:

Hardware

- **Hardware Installation:** Install your appliance hardware (physical appliances) using the [Stealthwatch x2xx Series Hardware Installation Guide](#) before you start this configuration.

- **Hardware Installation with a Data Store:** If you are deploying Stealthwatch with a Data Store, install your appliance hardware (physical appliances) using the [Stealthwatch x2xx Series Hardware (with Data Store) Installation Guide](#) before you start this configuration. Also, follow the [Stealthwatch Data Store Hardware Deployment and Configuration Guide](#) to properly configure your appliances for Data Store before you start this configuration.

- **Specifications:** [Hardware specifications](#) are available on Cisco.com.

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

Virtual Edition (VE) Appliances

- **Virtual Edition Installation:** Install your virtual appliances using the [Stealthwatch Virtual Edition Installation Guide](#) before you start this configuration.

- **Virtual Edition with Data Store Installation:** If you are deploying Stealthwatch Virtual Edition with a Data Store, install your virtual appliances using the [Stealthwatch Virtual Edition (with Data Store) Installation Guide](#) before you start this configuration. Also, follow the [Stealthwatch Data Store Virtual Edition Deployment and Configuration Guide](#) to properly configure your appliances for Data Store before you start this configuration.
Configuration Details

The system configuration includes the following:

- **Configuration Order:** Make sure you configure the appliances following the instructions in this guide and using the specified order.
- **Certificates:** Appliances are installed with a unique, self-signed appliance identity certificate.
- **Central Management:** You can manage your appliances from the primary SMC/Central Manager.

Downloading Software

Use Cisco Software Central to download virtual appliance (VE) installation files, patches, and software update files. Log in to your Cisco Smart Account at https://software.cisco.com or contact your administrator.

Licensing

For licensing Stealthwatch, you will use your Smart Account to register your product instance, manage licenses, run reports, and configure notifications. Log in to your Cisco Smart Account at https://software.cisco.com or contact your administrator.

When you use Stealthwatch in Evaluation mode, you can use selected features for 90 days. To use Stealthwatch with maximum default functionality, and to add licenses and features to your account, register your product instance for Smart Software Licensing. Refer to 5. Licensing for more information.

⚠️ Make sure you register your product instance before the 90-day evaluation period expires. When the evaluation period expires, flow collection will stop. To start flow collection again, register your product instance.

TLS

Stealthwatch requires v1.2.

Third Party Applications

Stealthwatch does not support installing third party applications on appliances.

Browsers

Stealthwatch supports the latest version of Chrome, Firefox, and Edge.
Host Name
A unique host name is required for each appliance. We cannot configure 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.

Domain Name
A fully qualified domain name is required for each appliance. We cannot install an appliance with an empty domain.

NTP Server
- **Configuration:** At least 1 NTP server is required for each appliance.
- **Problematic NTP:** Remove the 130.126.24.53 NTP server if it is in your list of servers. This server is known to be problematic and it is no longer supported in our default list of NTP servers.

Time Zone
All Stealthwatch appliances use Coordinated Universal Time (UTC).

- **Virtual Host Server:** Make sure your virtual host server is set to the correct time.

⚠️ Make sure the time setting on the virtual host server (where you will be installing the virtual appliances) is set to the correct time. Otherwise, the appliances may not be able to boot up.
1. Configuring Stealthwatch

When you log in to the appliance for the first time, you will use the Appliance Setup Tool to configure your appliance so it is managed by your Stealthwatch Management Console (SMC).

Preparation

Before you start the configuration, review the instructions so you understand the appliance configuration order, best practices, and additional requirements.

Stealthwatch with a Data Store

If you are deploying a Data Store, make sure you review the prerequisite deployment and configuration requirements for your Stealthwatch appliances before using Appliance Setup Tool.

- **Hardware:** Follow the [Stealthwatch Data Store Hardware Deployment and Configuration Guide](#).
- **Virtual Edition:** Follow the [Stealthwatch Data Store Virtual Edition Deployment and Configuration Guide](#).

Appliance Setup Tool Requirements

- Confirm your firewalls and ACLs (Access Control List) will allow access.
- Gather the host name for the appliance and IP addresses for the following:
  - appliance
  - subnet mask
  - default and broadcast gateways
  - NTP and DNS servers
  - SMC IP address for Central Management

Managed

As part of the Appliance Setup Tool, you will configure your appliance to be managed by your primary Stealthwatch Management Console (SMC).

When your appliances are managed by your Stealthwatch Management Console (SMC), you can use Central Management to edit appliance configurations, update software, reboot, shut down, and more.
SMC Failover

If you have more than one Stealthwatch Management Console (SMC), you can set up an SMC failover pair so that one of them serves as backup console to the other.

- Use the Appliance Setup Tool to configure each individual SMC.
- Plan which SMC will be primary and secondary.
- You can define the SMC failover relationship after you configure both SMCs and finish the system configuration. Refer to Defining an SMC Failover Relationship for details.

Best Practices

To configure your system successfully, make sure you follow the instructions in this guide. Make sure you review the following:

- **One at a Time:** Configure one appliance at a time. Confirm the appliance is **Up** before you start configuring the next appliance in your cluster.
- **Order:** Follow the appliance configuration order.
- **Multiple Central Managers:** You can configure more than one Central Manager in your system. However, each appliance can be managed by only one primary SMC/Central Manager.
- **Access:** You need administrator privileges to access Central Management.
Appliance Configuration Order

Configure your appliances in the following order, and note the details for each appliance:

<table>
<thead>
<tr>
<th>Order</th>
<th>Appliance</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Primary SMC</td>
<td>Your primary SMC is your Central Manager. Make sure the SMC is shown as Up before you start configuring the next appliance in the system.</td>
</tr>
<tr>
<td>2.</td>
<td>UDP Directors (also known as FlowReplicators)</td>
<td>If you are deploying a Data Store with your Stealthwatch deployment, see the Stealthwatch Data Store Hardware Deployment and Configuration Guide or the Stealthwatch Data Store Virtual Edition Deployment and Configuration Guide for more information on properly deploying and configuring your SMC for Data Store compatibility.</td>
</tr>
<tr>
<td>3.</td>
<td>All Data Nodes</td>
<td>See the Stealthwatch Data Store Hardware Deployment and Configuration Guide or the Stealthwatch Data Store Virtual Edition Deployment and Configuration Guide for more information on deployment and initializing your Data Store Vertica database.</td>
</tr>
<tr>
<td>4.</td>
<td>Flow Collector 5000 Series Database</td>
<td>Make sure the Flow Collector 5000 series database is shown as Up before</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>1.</td>
<td></td>
<td>Configuring Stealthwatch</td>
</tr>
<tr>
<td>5.</td>
<td>Flow Collector 5000 Series Engine</td>
<td>Make sure the Flow Collector 5000 series database is shown as Up before you start the engine configuration.</td>
</tr>
<tr>
<td>6.</td>
<td>All Other Flow Collectors (NetFlow and sFlow)</td>
<td>If you are deploying a Data Store with your Stealthwatch deployment, see the Stealthwatch Data Store Hardware Deployment and Configuration Guide or the Stealthwatch Data Store Virtual Edition Deployment and Configuration Guide for more information on properly deploying and configuring your Flow Collector for Data Store compatibility.</td>
</tr>
<tr>
<td>7.</td>
<td>Flow Sensors</td>
<td>Make sure your Flow Collector is shown as Up before you start the Flow Sensor configuration.</td>
</tr>
<tr>
<td>9.</td>
<td>Secondary SMC (if used)</td>
<td>Make sure the primary SMC is shown as Up before you start the secondary SMC configuration. The secondary SMC selects itself as Central Manager. Configure Failover after all appliances are configured. Refer to Defining an SMC Failover Relationship for details.</td>
</tr>
</tbody>
</table>

Your system might not have all the appliances shown here.
1. Log In

Use the following instructions to configure each appliance using the Appliance Setup Tool.

1. In the address field of your browser, type https:// followed by the IP address of the appliance.
   - **Primary SMC:** Configure the primary SMC first.
   - **Up:** Confirm each appliance is Up before you start configuring the next appliance in your cluster.
   - **Order:** Make sure you configure your appliances in order so they communicate correctly.

If you cannot access the appliance, please refer to the Configuring your Environment using First Time Setup: Troubleshooting instructions in your Stealthwatch hardware or Virtual Edition installation guide.

2. Enter the following credentials to log in:
   - **User Name:** admin
   - **Password:** lan411cope
2. Configure the Appliance

When you log in to the appliance for the first time, the Appliance Setup Tool guides you through each configuration step.

⚠️ If this is not a first-time installation, go to Troubleshooting to change appliance network settings such as host name, network domain name, or IP address.

1. **Change Default Password**: Enter new passwords for admin, root, and sysadmin. Click Next to scroll to each user.

   Use the following criteria:

   - **Length**: 8 to 256 characters
   - **Change**: Make sure the new password is different from the default password by at least 4 characters.

<table>
<thead>
<tr>
<th>User</th>
<th>Default Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>lan411cope</td>
</tr>
<tr>
<td>root</td>
<td>lan1cope</td>
</tr>
<tr>
<td>sysadmin</td>
<td>lan1cope</td>
</tr>
</tbody>
</table>
The sysadmin and root menus are unavailable if you've already changed the default passwords during the hardware installation. Refer to the Stealthwatch x2xx Series Hardware Installation Guide or Stealthwatch x2xx Series Hardware (with Data Store) Installation Guide for details.

2. **Management Network Interface**: Review the IP address and network interface fields. Confirm the default settings are correct. Click Next.

   - **Changes**: To change this information, confer with your network administrator and refer to Troubleshooting.
   - **IPv6 (optional)**: To enable IPv6, click IPv6. Check the Enable IPv6 check box and complete the fields.
3. **Host Name and Domains**: Enter the host name and network domain name. Click Next.

   - **Host Name**: A unique host name is required for each appliance. If you assign the same host names to your appliances, they will not install successfully.

     Also, make sure each appliance host name meets the Internet standard requirements for Internet hosts.

   - **Network Domain**: A fully qualified domain name is required for each appliance.

   - **Stealthwatch Domain (SMC only)**: Enter a Stealthwatch domain for your Stealthwatch appliances.

   - **IP Address Ranges (SMC only)**: Select the IP address range for your Stealthwatch network.

4. **DNS Settings**: Confirm the default is correct, or enter your domain server IP address. Click Next.
Add or Delete DNS Servers (optional):

- **Add**: Click the + icon.
- **Delete**: Click the check box to select the DNS server. Click the - icon.

5. **NTP Settings**: Confirm the default is correct, or click the Menu icon to select your network time protocol (NTP) server. Click Next.

- **Multiple NTP Servers**: We recommend setting up multiple NTP servers for redundancy and accuracy.
- **Public Source**: pool.ntp.org is a good, public source for NTP.

Add or Delete NTP Servers (optional):

- **Add**: Click the + icon.
- **Delete**: Click the check box to select the NTP server. Click the - icon.

6. If the appliance is an SMC, go to 3. **Register the Stealthwatch Management Console**.

   If the appliance is not an SMC, go to 4. **Add Appliances to Central Management**.
3. Register the Stealthwatch Management Console

1. **Review Your Settings**: Confirm the appliance information is accurate.
2. Click **Apply** or **Restart and Proceed**.

   Follow the on-screen prompts while the appliance restarts.

   Wait a few minutes for your new system settings to take effect. You may need to refresh the page.

3. Log in to the Stealthwatch Management Console.
4. The Appliance Setup Tool opens again. Click **Continue**.
5. On the Register Your Appliance tab, review the IP address and click **Save**.

   - This installs Central Management on the Stealthwatch Management Console.
   - The SMC IP address is detected automatically and cannot be changed.

6. When the appliance setup is completed, click **Go to Dashboard**.
7. Click the **Global Settings** icon. Select **Central Management**.
8. Review the inventory. Confirm the SMC appliance status is shown as Up.

![Image of inventory status]

Make sure the primary SMC and each appliance is shown as Up before you start configuring the next appliance in your cluster using the configuration order and details.

9. To configure the next appliance in your system, go to 1. Log In, and complete the procedures through 5. Confirm Appliance Status.

If you don’t have another appliance to set up, go to 2. Finishing Appliance Configurations.

4. Add Appliances to Central Management

The Appliance Setup Tool continues to guide you through the appliance configuration with Central Management. Some of the steps may vary depending on the appliance. Follow the on-screen prompts.

1. On the Central Management tab, enter the IP address of your primary SMC.

   Your primary SMC is your Central Manager.

2. Click Save.

3. Follow the on-screen prompts to trust the primary SMC appliance identity certificate. Click Yes to trust the certificate and allow the appliance to communicate with the SMC.

4. Enter the login credentials for your primary SMC.

5. Select your Stealthwatch Domain.
- **Flow Collectors**: Enter the Flow Collection port number.

  Netflow Default: 2055  
sFlow Default: 6343  

- **Flow Sensors**: Select a Flow Collector.

6. Click **Go to Central Management**. Go to **5. Confirm Appliance Status**.
5. Confirm Appliance Status

After you configure an appliance in the Appliance Setup Tool, confirm the appliance status in Central Management.

1. The Appliance Setup Tool opens to the Central Management inventory, or you can open it as follows:
   - Log in to your primary Stealthwatch Management Console.
   - Click the Global Settings icon.
   - Select Central Management.

2. Review the appliances on the Appliance Manager inventory.
   - Confirm the appliance is shown in the inventory.
   - Confirm the status for the appliance is shown as Up.

![Inventory of appliances in Stealthwatch Central Management](image)

Make sure the primary SMC and each appliance is shown as Up before you start configuring the next appliance in your cluster using the configuration order and details.

3. To configure the next appliance in your system, go to 1. Log In, and complete the procedures through 5. Confirm Appliance Status.
If you don't have another appliance to set up, go to 2. Finishing Appliance Configurations.
2. Finishing Appliance Configurations

Use the following instructions to finish configuring each appliance.

Depending on the speed of your VM host, it may take approximately 30 minutes for all services to boot up.

1. Click the link for the appliance you are configuring:

<table>
<thead>
<tr>
<th>Appliance</th>
<th>Required Configurations</th>
<th>Optional Configurations</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMC</td>
<td>If you are not deploying a Data Store with your Stealthwatch deployment, no additional configuration is required. If you are deploying a Data Store with your Stealthwatch deployment, see the Stealthwatch Data Store Hardware Deployment and Configuration Guide or the Stealthwatch Data Store Virtual Edition Deployment and Configuration Guide for more information on completing your Stealthwatch deployment.</td>
<td>n/a</td>
</tr>
<tr>
<td>Flow Collector</td>
<td>If you are not deploying a Data Store with your Stealthwatch deployment, no additional configuration is required. If you are deploying Stealthwatch with a Data Store, see the Stealthwatch Data Store Hardware Deployment and Configuration Guide or the Stealthwatch Data Store Virtual Edition Deployment and</td>
<td>n/a</td>
</tr>
<tr>
<td>Appliance</td>
<td>Configuration</td>
<td>Feature</td>
</tr>
<tr>
<td>------------------</td>
<td>----------------------------------------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>Data Node</td>
<td><strong>Configuration Guide</strong> for more information on completing your Stealthwatch deployment.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>See the <a href="#">Stealthwatch Data Store Hardware Deployment and Configuration Guide</a> or the <a href="#">Stealthwatch Data Store Virtual Edition Deployment and Configuration Guide</a> for more information on deploying and initializing your Data Store database, configuring Vertica Management Console, and configuring Data Store data retention period.</td>
<td></td>
</tr>
<tr>
<td>UDP Director</td>
<td>High Availability (available on hardware only)</td>
<td></td>
</tr>
<tr>
<td>Flow Sensor</td>
<td>Application ID and Payload</td>
<td>Identifying Applications</td>
</tr>
</tbody>
</table>

2. When you are finished configuring and restarting each appliance in the table, go to **3. Installing the Stealthwatch Desktop Client**.
UDP Director

Use the following instructions to finish configuring the UDP Director.

- **Forwarding Rules**: Configure at least one forwarding rule if you’re planning to set up High Availability. Refer to Configuring Forwarding Rules
- **High Availability**: If you have more than one UDP Director, you can set up a High Availability pair. Configure at least one forwarding rule if you’re planning to set up High Availability (refer to Configuring High Availability).

**Configuring Forwarding Rules**

SSL is used to send messages from the UDP Director to the Stealthwatch Management Console (SMC).

1. Log in to the SMC.
2. Click the Global Settings icon. Select UDP Director Configuration.

3. Click the Actions menu for the appliance. Select Configure Forwarding Rules.
4. Click Add New Rule.
5. **Description**: Enter a brief description that identifies the rule.
6. **Source IP Address:Port**: Type the IP address of the device that sends data to the UDP Director and the input port number (where the data will be sent).
   - **Format**: Use the syntax [IP address]:[Port Number].
- **Range:** You can use Classless Inter-Domain Routing (CIDR) notation to enter a range of IP addresses.

- **All:** You can type "All" to accept data from any source IP address on this port.

- **Combinations:** You can add Source IP Address:Port combinations within a rule by adding them to a new line.

**Examples:**

- 10.11.16.38:5322
- 192.168.0.0/16:9000
- All:2055

7. **Destination IP Address:** Enter the IP address of the device receiving data from the UDP Director.

8. **Destination Port Number:** Enter the port number for the receiving device.

9. Click **Save**.

10. **Optional:** To sync your changes, click Sync.

11. Repeat the procedure to add forwarding rules as needed.

12. To set up a High Availability pair, go to **Configuring High Availability**.

   **Info:** High Availability is only available on UDP Director hardware appliances. High Availability is not available on virtual appliances.

   If you do not need to set up a High Availability pair, return to **2. Finishing Appliance Configurations**.

**Configuring High Availability**

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

**Info:** High Availability is only available on UDP Director hardware appliances. High Availability is not available on virtual appliances.

The UDP Director High Availability allows a user to configure settings for redundant UDP Directors. Both nodes are fully redundant, however only one node is online at a time.
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 HA 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 Stealthwatch system, log in to the secondary UDP Director and configure its HA components as described here.

1. **Configure the Primary UDP Director HA**

   1. Log in to the primary UDP Director Appliance Admin interface.
   2. Click **Configuration > High Availability**.
   3. Check the **Enable High Availability Service** check box for the High Availability Settings.
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.

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.

   Each of the IP addresses—eth0, eth02, eth03—must be on its own separate unicast subnet.
8. After reviewing the setting, click Apply to set the configuration.
9. Continue to the next section to configure the second UDP Director of the cluster.

2. Configure the Secondary UDP Director HA

To configure the secondary UDP Director complete the following steps:

1. Log in to the secondary UDP Director Appliance Admin interface.
2. Click Configuration > High Availability.
3. 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.
4. Click Apply to save your changes and to start the clustering services on this appliance.
5. Click Promote to designate the primary appliance.
Flow Sensor

1. Configure the Application ID and Payload

The configuration of a Flow Sensor requires an additional step of configuring the application ID and payload.

1. Log in to the Flow Sensor Appliance Admin interface.
2. Click Configuration > Advanced Settings.

The Advanced Settings page opens.

3. Select the proper settings for your network:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export Packet Payload</td>
<td>Allows you to specify whether the Flow Sensor includes the first 26 bytes of binary payload data in the data that it sends to the collector.</td>
</tr>
<tr>
<td>Export Applications Identification</td>
<td>Allows you to specify whether the Flow Sensor attempts to identify applications before sending data to the collector. In addition, this setting must be enabled for the following settings to take affect:</td>
</tr>
<tr>
<td></td>
<td>Include IPv6 – Allows you to specify whether or not the Flow Sensor analyzes both IPv4 and IPv6 packets. When this setting is disabled, the Flow Sensor analyzes only IPv4 packets.</td>
</tr>
<tr>
<td></td>
<td>Export HTTPS Header Data – Allows you to specify whether the Flow Sensor includes header data from HTTPS flows in the data that it sends to the collector. The data includes the SSL common name and SSL organization name. This setting requires that the Flow Type is set to IPFIX. The maximum is 256 bytes.</td>
</tr>
<tr>
<td></td>
<td>Export HTTP Header Data – Allows you to specify whether or not the Flow Sensor includes header data from HTTP flows in the data that it sends to the collector. When this setting is selected, a secondary field allows you to specify the maximum length of the HTTP path (in bytes) that the Flow Sensor includes as part of the flow data. This setting requires that the Flow Type is set to IPFIX.</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Enable VXLAN Decapsulation</td>
<td>Allows you to specify whether the Flow Sensor uses Virtual Extensible Local Area Network (VXLAN) decapsulation capabilities. Without VXLAN decapsulation, the Flow Sensor simply detects VXLAN encapsulated traffic as flows between two Virtual Tunnel Endpoints (VTEPs). Decapsulation allows for much richer content by being able to analyze the tunneled traffic and thus gain greater insight into the traffic patterns in the network.</td>
</tr>
<tr>
<td></td>
<td>The Flow Sensor will only decapsulate VXLAN traffic which was originally sent to the standard VXLAN port (4789).</td>
</tr>
<tr>
<td>Enable GENEVE Decapsulation</td>
<td>Allows you to specify whether the Flow Sensor uses Generic Network Virtualization Encapsulation (GENEVE) decapsulation for traffic received on its monitoring ports.</td>
</tr>
<tr>
<td>Enable ERSPAN Decapsulation</td>
<td>Allows you to specify whether to Flow Sensor uses Encapsulated Remote Switching Port Analyzer (ERSPAN) decapsulation capabilities to detect the ERSPAN header in packets, and then decapsulate the header and process the inner packet contents. You are required to assign the monitoring interface an IP address to allow termination of the ERSPAN tunnel on the Flow Sensor. ERSPAN decapsulation is not supported on the FS 4210.</td>
</tr>
<tr>
<td>Enable X-Forwarded-For Processing</td>
<td>Allows you to specify whether the Flow Sensor uses X-Forwarded-For (XFF) processing to identify the originating IP address of a client connecting to a web server through an HTTP proxy or a load balancer. ETA and X-Forwarded-For Processing cannot be configured together.</td>
</tr>
<tr>
<td>Enable ETA Processing</td>
<td>Allows you to specify whether the Flow Sensor uses ETA processing to generate and transmit IDP and SPLT fields to your SMC.</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Enabling ETA</strong> increases NetFlow bandwidth usage, especially when using v9. We recommend using IPFIX for the Flow Export Format.</td>
<td></td>
</tr>
<tr>
<td>ETA and X-Forwarded-For Processing cannot be configured together.</td>
<td></td>
</tr>
<tr>
<td>ETA cannot be enabled on Dell or PowerEdge Flow Sensor models.</td>
<td></td>
</tr>
<tr>
<td><strong>Enable Load Balancing</strong></td>
<td>Allows you to specify whether the Flow Sensor 4000 series can distribute flow data to more than one Flow Collector. Use this option if the flow data from the Flow Sensor exceeds the capacity of one Flow Collector.</td>
</tr>
<tr>
<td><strong>Monitoring Interface Selection</strong></td>
<td>Allows you to specify whether the Flow Sensor 4240 uses 2 x 40G or 4 x 10G (SFP) interfaces. You must be using multiple Flow Collectors and have Load Balancing enabled for this setting to work properly. Go to the <a href="#">Flow Sensor and Load Balancer Integration Guide</a> for more information. This option is only available on the Flow Sensor 4240. The default setting is 2 x 40G.</td>
</tr>
</tbody>
</table>
| **Cache Mode** | Allows you to select one of the following settings: Use single, shared, cache for all monitoring ports –  
  - Use when asymmetric routing is present.  
  - Single state table for application and latency calculations.  
  - Uses less memory.  
  - Lower overall pps processing rates.  
  - Results in one NetFlow event created across multiple interfaces. |
<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Use only when the Flow Sensor has only two ports and is connected by a TAP</td>
</tr>
<tr>
<td></td>
<td>Use independent caches for each monitoring port –</td>
</tr>
<tr>
<td></td>
<td>• Allows deduplication of packets across each Flow Sensor interface.</td>
</tr>
<tr>
<td></td>
<td>• Uses more memory.</td>
</tr>
<tr>
<td></td>
<td>• Higher overall pps processing rates.</td>
</tr>
<tr>
<td></td>
<td>• Each interface maintains its own latency and application database.</td>
</tr>
<tr>
<td></td>
<td>• Results in a unique NetFlow record for each interface that sees a given packet.</td>
</tr>
</tbody>
</table>

4. Click **Apply** to save your settings.

2. **Configure the Flow Sensor to Identify Applications (optional)**

If you want the Flow Sensor to identify applications, configure the following settings:

1. Log in to the Flow Sensor Appliance Admin interface.
2. Click **Configuration > Advanced Settings**
3. Check the **Export Application Identification** check box. By default, this option is not selected.
4. If you have more than 1 monitoring NIC, select one of the following options in the **Cache Mode** section:
   - **Use single, shared, cache for all monitoring ports**: typically used for systems that monitor flows using the TAP method.
   - **Use independent caches for each monitoring port**: typically used to experience better performance and for systems that monitor flows using the SPAN method.
3. Restart the Appliance

3. Installing the Stealthwatch Desktop Client

If you deployed Stealthwatch with a Data Store, you will not use the Stealthwatch Desktop Client.

Use the following instructions to install the Stealthwatch Desktop Client using Windows or macOS. Note the following:

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

Install the Desktop Client Using Windows

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

1. Log in to your SMC.
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 Stealthwatch Desktop Client.
5. On your desktop, click the Stealthwatch Desktop Client icon 📀.
6. Enter the SMC user name and password.
7. Enter the SMC server name or IP address (IPv4 or IPv6).
8. Follow the on-screen prompts to open the Desktop Client and trust the appliance identity certificate.

**Change the Memory Size**

You can change how much Random Access Memory (RAM) to allocate on your client computer to run the Stealthwatch Desktop Client interface. Consider a larger memory allocation if you work with many open documents or large data sets (such as flow queries with over 100k records).

1. In Windows Explorer, go to your home directory.
2. Open these folders: AppData > Roaming > Stealthwatch.
   
   You may need to search "Stealthwatch" if the folder is hidden.
3. In the Stealthwatch directory, open the folder that contains the desired Stealthwatch version.
4. Open the *application.vmoptions* file using an appropriate editing application to begin editing. (This file is created after you open the Stealthwatch Desktop Client for the first time.)

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

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

```
# 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 Stealthwatch Desktop Client appears to "hang" frequently, try increasing the memory size.

If you receive an error message involving Java, try selecting a lower memory allocation.

Install the Desktop Client Using macOS

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

1. Log in to your SMC.
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 Stealthwatch Desktop Client icon (❖) into the Application folder.
   The icon is added to the Launchpad.

5. On your desktop, click the Stealthwatch Desktop Client icon (❖).
6. Enter the SMC user name and password.
7. Enter the SMC server name or IP address (IPv4 or IPv6).
8. Follow the on-screen prompts to open the Desktop Client and trust the appliance identity certificate.

© 2021 Cisco Systems, Inc. and/or its affiliates. All rights reserved.
Change the Memory Size

You can change how much Random Access Memory (RAM) to allocate on your client computer to run the Stealthwatch Desktop Client interface. Consider a larger memory allocation if you work with many open documents or large data sets (such as flow queries with over 100k records).

1. In Finder, go to your home directory.
2. Open the Stealthwatch folder.
3. In the Stealthwatch directory, open the folder that contains the desired Stealthwatch version.
4. Open the application.vmoptions file using an appropriate editing application to begin editing. (This file is created after you open the Stealthwatch Desktop Client for the first time.)

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

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

```
# 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
```

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.
-Xmx512m
```

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

- If you notice that the Stealthwatch Desktop Client appears to "hang" frequently, try increasing the memory size.
- If you receive an error message involving Java, try selecting a lower memory allocation.
4. Verifying Communications

Use the following instructions to confirm the Stealthwatch Management Console is receiving NetFlow data.

If you deployed Stealthwatch with a Data Store, see the Stealthwatch Data Store Hardware Deployment and Configuration Guide or the Stealthwatch Data Store Virtual Edition Deployment and Configuration Guide to verify communications.

Verify NetFlow Data Collection

1. In the Stealthwatch Desktop Client Enterprise tree, right-click the Flow Collector. Select Status > NetFlow Collection Status.

2. On the NetFlow Collection Status page, look at the Current NetFlow Traffic field located at the top of the document. This statistic shows the amount of NetFlow traffic being observed.
   - If traffic is shown, go to the next step.
   - If traffic is not shown, check your exporter/router configurations. For details, refer to the SMC Client Online Help. Then, go to the next step.
3. Look at the **Longest Duration Export** column.

   **Add Column:** To add this column to your dashboard, right-click a column heading and select **Longest Duration Export** from the menu.

4. Is the value for each exporter below 100?
   - If yes, the cache export timer is fine.
   - If no, higher values indicate an incorrect cache export timer, which may result in unrealistic alarms. Check your exporter/router configurations. For details, refer to the SMC Client Online Help.

5. Congratulations! You are finished with your Stealthwatch system configuration.

6. **Next Steps:** Review 5. **Licensing**, and register your product instance in your Cisco Smart Account before the evaluation period expires.

   - Make sure you register your product instance before the 90-day evaluation period expires. When the evaluation period expires, flow collection will stop. To start flow collection again, register your product instance.

7. To add more services and features to Stealthwatch, refer to the following resources:
   - Defining an SMC Failover Relationship
   - Enabling the Threat Intelligence Feed
   - Configuring SAML SSO
Refer to Cisco.com to review our Stealthwatch guides and configure additional features such as Cisco Threat Response, Cisco Identity Services (ISE), TACACS+, and more.

To start using Stealthwatch, refer to the following sections of this guide:

- **Getting Started**: Review the Getting Started with Stealthwatch section for more information about managing your environment, investigating behavior, responding to threats, and more.

- **Central Management**: Refer to the Central Management section in this guide for more information about managing your appliances and changing configuration settings.

- **Troubleshooting**: Refer to the Troubleshooting section of this guide.
5. Licensing

Use Cisco Smart Software Licensing to license your Stealthwatch appliances and features. For more information, refer to Smart Licensing on cisco.com.

- **Online:** To use Smart Licensing and Stealthwatch online, please refer to the Stealthwatch Smart Software Licensing Guide. You need Internet access for this configuration.
- **Offline:** To discuss your licensing options for closed/airgap networks, contact Cisco Stealthwatch Support.
- **Cisco Smart Account:** To set up a Cisco Smart Account, register at https://software.cisco.com or contact your administrator.

**Evaluation Mode**

When you use Stealthwatch in Evaluation mode, you can use selected features for 90 days. To use Stealthwatch with maximum default functionality, and to add licenses and features to your account, register your product instance for Smart Software Licensing.

⚠️ Make sure you register your product instance before the 90-day evaluation period expires. When the evaluation period expires, flow collection will stop. To start flow collection again, register your product instance.

- **Admin User:** To review Smart Licensing status and usage details in your Stealthwatch Management Console, log in as the admin user.
- **Days Remaining:** To review the days remaining in Evaluation Mode, log in to the Stealthwatch Management Console as the admin user. Go to Central Management > Smart Licensing. Review the License Authorization Status.
- **Product Instance:** The Product Instance Name is the identifier we use for your Stealthwatch product instance, which includes your Stealthwatch Management Console and managed appliances.
Defining an SMC Failover Relationship

Use Failover Configuration to establish a failover pair between two Stealthwatch Management Consoles (SMCs) so that one of them serves as a backup console to the other.

For a successful configuration and operation, review the requirements and follow the instructions in the Stealthwatch Failover Configuration Guide.

If your primary SMC goes offline, please note that the SMCs do not swap roles automatically. Make sure you change the SMC roles in the order shown in the Stealthwatch Failover Configuration Guide.

Configuring Failover

To configure your SMCs as a failover pair, follow the instructions in the Stealthwatch Failover Configuration Guide.

The guide includes details that are critical for a successful configuration, including:

- **Certificates**: To set up trust between appliances so they can communicate, make sure you save the correct certificates to the required appliance Trust Stores.
- **Backup Files**: Back up the appliances before you start the failover configuration.
- **Configuration Order**: You will configure the secondary SMC for failover before you configure the primary SMC.
- **Changing Roles**: If your primary SMC goes offline, make sure you change the SMC roles in the order shown in the guide. The order is critical, and they do not swap roles automatically.
- **Troubleshooting**: Refer to the Stealthwatch Failover Configuration Guide for solutions.

For a successful configuration and operation, follow the instructions in the Stealthwatch Failover Configuration Guide.

Primary and Secondary Roles

As part of the configuration, you will assign a primary SMC and a secondary SMC. When you save the configuration, the following occurs:

- **Primary SMC**: The primary SMC pushes its domain configuration, user settings, and policies to the secondary SMC. Use the primary SMC to manage your appliances, change appliance configurations, change passwords, define alarms, apply policies,
and more.

- **Secondary SMC**: The secondary SMC deletes its configuration, so it can synchronize with the primary SMC configuration and settings. Also, the secondary SMC changes to read-only for all users, which means that you will not have access to sections of the secondary SMC and you cannot retrieve files from the secondary SMC.
Enabling the Threat Intelligence Feed

The Threat Intelligence Feed provides data from the global threat intelligence feed about threats to your network. The feed updates frequently and includes IP addresses, port number, protocols, host names, and URLs known to be used for malicious activity. The following host groups are included in the feed: command-and-control servers, bogons, and Tors.

License

Add the Threat Intelligence Feed License to your Cisco Smart Account. For instructions, refer to the Stealthwatch Smart Software Licensing Guide.

Enable

To enable the feed in Central Management, follow the instructions in the online help. Please note that you will configure the DNS server and firewall as part of the instructions.

1. Log in to your primary Stealthwatch Management Console.
2. Click the Global Settings icon.
3. Select Central Management.
4. Click the User icon. Select Stealthwatch Online Help.
5. Select Appliance Configuration > Threat Intelligence Feed.

Review Alarms and Security Events

When the Threat Intelligence Feed is enabled, the Stealthwatch Labs Intelligence Center icon is shown in the Stealthwatch Desktop Client Enterprise tree with an alarms status, and threats are displayed in their respective host group branches. For more information, refer to the Stealthwatch Desktop Client User Guide or the online help.

Online Help: To access the Online Help, right-click the Stealthwatch Labs Intelligence Center branch and select Configuration > SLIC Threat Feed Configuration. Click Help.
Enabling the Threat Intelligence Feed
Configuring SAML SSO

Use the following instructions to configure Security Assertion Markup Language Single Sign-On (SAML SSO). SSO is an authentication process that allows a user to access multiple applications with one set of credentials.

Support Details

Please note the following configurations are supported or not supported.

<table>
<thead>
<tr>
<th>Supported</th>
<th>Not Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Active Directory Federation Services (ADFS) for SAML/SSO</td>
<td>Stealthwatch Desktop Client</td>
</tr>
<tr>
<td>On-Premise solutions of Microsoft ADFS</td>
<td>Cloud Services of Microsoft ADFS</td>
</tr>
<tr>
<td></td>
<td>Integrated Windows Authentication (IWA)</td>
</tr>
<tr>
<td></td>
<td>Additional Proxies</td>
</tr>
<tr>
<td></td>
<td>External Services</td>
</tr>
</tbody>
</table>

1. Prepare for Configuration

You need the following information to configure SSO:

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Provider URL</td>
<td>The URL must use the fully qualified domain name or IPv4 address.</td>
</tr>
<tr>
<td>Identity Provider Certificate</td>
<td>If the IDP URL starts with HTTPS, download the CA certificate.</td>
</tr>
</tbody>
</table>
2. Upload Certificates to the Trust Store

If the Identity Service Provider (IDP) URL starts with HTTPS, add the root CA certificate to the SMC Trust Store.

If the IDP URL does not start with HTTPS, you can skip this step and go to the next section, 3. Configure the Service Provider.

Use the following instructions to add the root CA certificate to the SMC Trust Store.

1. On the Central Management Appliance Manager page, click the Actions menu for the SMC.
2. Select Edit Appliance Configuration.
3. On the Appliance Manager > General tab, locate the Trust Store section.
4. Click Add New.
5. In the Friendly Name field, enter a name for the certificate.
6. Click Choose File. Select the new certificate.
7. Click Add Certificate. Confirm the new certificate is shown in the Trust Store list.
8. Click Apply Settings. Follow the on-screen prompts.
9. Up: On the Appliance Manager page, make sure the SMC finishes the configuration changes and the Appliance Status returns to Up.

Do not force the appliance to reboot while configuration changes are pending.

10. If you have a secondary SMC, repeat this procedure to add the root CA certificate to the secondary SMC Trust Store.
11. If you have added the root CA certificate to the SMC Trust Stores, go to the next section.

3. Configure the Service Provider

1. Log in to the SMC console as root.
2. Type SystemConfig. Press Enter.
3. Select Advanced
4. Select SSO.
5. Confirm ssoEnable/Disable is shown as Disabled.
6. Select **IdentityProvider (IDP)**. Click **Continue**.

7. Enter the URL where the Identity Provider's configuration file can be downloaded.

   **Requirements:** Enter the fully qualified domain name or IPv4 address.

8. Select **DownloadIDP**. Follow the on-screen prompts to enable it.

9. Select **SaveChanges**. Click **Continue**.

   Follow the on-screen prompts to download the IDP configuration file.

10. Select **SSO**.

11. Review **ServiceProvider (SP)**. Copy the URL. You will use it to configure the identity provider.

12. Review **Status**. Confirm it is shown as **Ready**.
4. Enable SSO

1. Select ssoEnable/Disable.
2. Follow the on-screen prompts to enable SSO.
3. Select CredentialDescription. Click Continue.
4. Enter a description of the SSO service credentials users need to log in.
5. Click OK.
6. Select DownloadIDP. Disable DownloadIDP until you need to save a new SSO configuration.
   - Click Continue.
   - Follow the on-screen prompts to disable DownloadIDP.
7. Select SaveChanges. Click Continue.
8. Exit System Configuration.

5. Configure the Identity Provider

1. In the address field of your browser, type the Service Provider URL.
2. Download the Service Provider metadata file sp.xml.
3. Configure the Identity Provider with sp.xml.
4. Make sure the outgoing claim type includes the user email address.

   - For example: If the Attribute store is the Active Directory, set the outgoing claim type to the email address for the LDAP Attribute type user ID.
   - Microsoft Active Directory Federation Services (ADFS): If the IDP type is ADFS, confirm the following custom rule is shown:

```c:
[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"] => issue
(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer = c.Issuer, Value = c.Value, ValueType = c.ValueType, Properties
6. Add an SSO User

Use the following instructions to add an SSO user. Users are authenticated through/by the Identity Provider.

1. Log in to the SMC (Stealthwatch Web App).
2. Click the Global Settings icon.
4. Select Create > User.

For instructions, click the User icon. Select Stealthwatch Online Help. For details about adding users, refer to "Configuring Users."

5. Complete the fields to create a new user. Configure the user as follows:
   - Authentication Service: Select SSO.
   - User Name: Enter the first part of the email address for the IDP account. Make sure the ID is identical to the one that will be used for SSO at login. For example, for name@cisco.com, enter "name" in this field.

6. Click Save.
7. Confirm the SSO User is shown in User Management.

7. Test SAML Login

1. Log in to the SMC (Stealthwatch Web App).
2. On the login page, click the drop-down.
3. Select SAML.
4. Click the credentials button.
5. Enter the login credentials. The SMC opens to the Security Insight Dashboard.
## Troubleshooting

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Lockout</td>
<td>Disable SSO Only from System Configuration through emergency account access.</td>
</tr>
<tr>
<td>Cannot download IDP XML</td>
<td>Make sure the IDP certificate is uploaded to the SMC Trust Store.</td>
</tr>
<tr>
<td>Cannot save IDP configuration</td>
<td>Review the IDP configuration and make sure the data you entered is accurate and doesn't include any extra spaces. Also, review the IDP event logs.</td>
</tr>
<tr>
<td>Additional Issues</td>
<td>Download a SAML tracer for your browser. Repeat the SSO login to review the exchanges between the IDP and SP.</td>
</tr>
</tbody>
</table>
Getting Started with Stealthwatch

After you have finished configuring your appliances, Stealthwatch Online Help provides instructions for managing your environment, investigating behavior, responding to threats, and more.

Overview

For an overview of Stealthwatch, review the information in Stealthwatch Online Help.

1. Click the User icon.
2. Select Stealthwatch Online Help.
3. At the top of the page, select the Stealthwatch Help menu.

Managing Your Environment

As part of managing your network security, you need to perform several preliminary tasks. The menus to access each page are shown with each topic below. For instructions, select the User icon > Stealthwatch Online Help from any page.

- Configuring host groups (Configure > Host Group Management)
- Creating and managing policies (Configure > Policy Management)
- Building flow searches (Analyze > Flow Search)
- Managing user permissions for using Stealthwatch (Global Settings icon > User Management)

Investigating Behavior

For information about investigating alarms, events, hosts, and more, review the information in Stealthwatch Online Help.

1. Click the User icon.
2. Select Stealthwatch Online Help.
3. At the top of the page, select the Stealthwatch Help menu.
4. Select Investigating Behavior.

Responding To Threats

For policy information, review the information in Stealthwatch Online Help.
1. Click the User icon.
2. Select Stealthwatch Online Help.
3. At the top of the page, select the Stealthwatch Help menu.
4. Select Responding to Threats.
Central Management

Use Central Management to manage your appliances from your primary SMC. We’ve included an overview of Central Management here, and details for each section are available in Stealthwatch Online Help.

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

- **Stealthwatch Online Help:** To open Stealthwatch Online Help, click the User icon. Select *Stealthwatch Online Help*

Central Management and Appliance Administration Interface

When an appliance is managed by Central Management, you will access functions for your appliance in Central Management and the Appliance Administration interface (Appliance Admin) as follows:

<table>
<thead>
<tr>
<th>Central Management</th>
<th>Appliance Admin Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit appliance configuration</td>
<td>View system statistics</td>
</tr>
<tr>
<td>Review license status (overview)</td>
<td></td>
</tr>
<tr>
<td>Back up configuration files</td>
<td>Back up database files</td>
</tr>
<tr>
<td>View audit logs</td>
<td>Create diagnostics packs</td>
</tr>
<tr>
<td>Reboot</td>
<td>Network Host and IP Lookup</td>
</tr>
<tr>
<td>Shut down</td>
<td>Packet Capture</td>
</tr>
<tr>
<td>Update software</td>
<td>Clearing the DNS Cache</td>
</tr>
<tr>
<td></td>
<td>Appliance-specific configurations</td>
</tr>
</tbody>
</table>
If you configure a Flow Collector for Data Store compatibility, the Appliance Administration interface (Appliance Admin) hides certain functionality. Use Central Management to configure the Flow Collector and other related tasks.

Opening Central Management

1. Log in to your primary SMC.
2. Click the Global Settings icon.
3. Select Central Management.

Opening Appliance Admin

You can access the Appliance Admin interface through Central Management or by logging in to the appliance directly.

Opening Appliance Admin through Central Management

1. On the Central Management Appliance Manager page, click the Actions menu for the appliance.
2. Select View Appliance Statistics.
3. Log in to the Appliance Administration interface.

Opening Appliance Admin through Direct Login

1. In your browser address bar, type the appliance IP address as follows:

   https://<IPAddress>
- **SMC**: add `/smc/index.html` after the IP address.
- **For example**: `https://1.1.1.1/smc/index.html`

2. Press Enter.

**Editing Appliance Configuration**

1. On the [Central Management](#) Appliance Manager page, click the **Actions** menu for the appliance.

2. Select **Edit Appliance Configuration**.

3. Click the **Configuration** menu. Select an item from the list.

   or

   Click each tab to review each configuration category.

4. Make changes to each configuration section as needed. You can edit more than one configuration category on each configuration tab.
5. Click **Apply Settings**. Follow the on-screen prompts to save your configuration changes.

Some changes require a system reboot. If you prefer to wait, you can revert your changes and edit your configuration settings and reboot later.

The appliance reboots automatically. Do not force the appliance to reboot while configuration changes are pending. To confirm the appliance status is Up, review Central Management > Appliance Manager inventory.

6. **Up**: On the Appliance Manager page, make sure the appliance finishes the configuration changes and the Appliance Status returns to **Up**.

**Viewing Appliance Statistics**

**Hover**: For more information about each appliance status, hover your pointer over the status.

To see system statistics, services, disk usage, and docker services, log in to the Appliance Admin interface:

1. On the **Central Management** Appliance Manager page, click the **Actions** menu for the appliance.
2. Select **View Appliance Statistics**.
3. Log in to the Appliance Administration interface.

**Removing an Appliance from Central Management**

Use the following instructions to remove an appliance from your Central Manager.

1. On the **Central Management** Appliance Manager page, click the **Actions** menu for the appliance.
2. Select **Remove This Appliance**.

**Config Channel Down**: If you're removing the appliance because the configuration channel is down, go to the **Config Channel Down** procedure in Troubleshooting for additional instructions.
Troubleshooting: If you log in to the Appliance Admin interface and the appliance is not removed from Central Management, go to the Config Channel Down procedure in Troubleshooting to remove it using System Configuration.

Central Management: To add the appliance to a different Central Manager, use the Appliance Setup Tool.

If your appliance has custom certificates, make sure you save the identity certificate and certificate chain (root and intermediate) to the SMC Trust Store before you add the appliance to Central Management. For instructions, refer to the SSL/TLS Certificates for Managed Appliances Guide.

Adding an Appliance to Central Management

Use the Appliance Setup Tool to add an appliance to Central Management. It is important to review the following:

- **Custom Certificates**: If your appliance has custom certificates, make sure you save the identity certificate and certificate chain (root and intermediate) to its own Trust Store and the SMC Trust Store before you add the appliance to Central Management. For instructions, refer to the SSL/TLS Certificates for Managed Appliances Guide.

- **SMC Administration Credentials**: You need the SMC, user ID and password to add an appliance to Central Management.

- **RFD**: If you reset the factory defaults on an appliance, configure the appliance IP address, host name, and domain before you add it to Central Management (even if you preserve network settings when you RFD).

Log in to the appliance console as **sysadmin** and follow the on-screen prompts to configure the IP address, host name, and domain. For instructions, refer to your Stealthwatch hardware or Virtual Edition installation guide.

- **New Installations**: If this is a new installation, make sure you complete the installation and configure the IP address, host name, and domain before you add it to Central Management. For instructions, refer to your Stealthwatch hardware or Virtual Edition installation guide.
If your appliance has custom certificates, make sure you save the identity certificate and certificate chain (root and intermediate) to the SMC Trust Store before you add the appliance to Central Management. Refer to the SSL/TLS Certificates for Managed Appliances Guide.

1. Log in to the Appliance Admin interface.

2. In the appliance browser address bar, after the IP address, replace the end of the URL with /lc-ast:

   https://<IP Address>/lc-ast

3. Press Enter.

4. Click Next to scroll to the Central Management tab.

5. IP Address: Enter the SMC/Central Manager IP address.

6. Click Save.

7. Follow the on-screen prompts to enter the SMC administration credentials and finish the configuration. Depending on the type of appliance, you may need to enter additional information.

8. For more information about the Appliance Setup Tool, refer to 1. Configuring Stealthwatch.

Enable/Disable SSH

Use this section to control the ability to access the appliance using SSH (secure shell).

Default: disabled

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

Open SSH

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

1. Open Central Management.
2. Click the Actions menu for the appliance.
3. Select Edit Appliance Configuration.
4. Select the Appliance tab.
Enable SSH

1. Locate the SSH section.
2. To allow SSH access on the appliance, check the Enable SSH check box.
3. To allow root access on the appliance, check the Enable Root SSH Access check box.
4. Click Apply Settings.
5. Follow the on-screen prompts.

Disable SSH

1. To remove SSH access on the appliance, click the Enable SSH check box to clear it.
2. To remove root access on the appliance, click the Enable Root SSH Access check box to clear it.
3. Click Apply Settings.
4. Follow the on-screen prompts.
Troubleshooting

Config Channel Down

If your Appliance Manager shows **Config Channel Down** for the appliance status, check the following:

- **Communication Settings:** Confirm your network communication settings.
- **Trust Stores:** Make sure your appliance identity certificates are saved to the correct Trust Stores. For instructions, refer to the [SSL/TLS Certificates for Managed Appliances Guide](#).
- **Certificates:** If you’ve changed the appliance identity certificate, check the procedure and confirm your certificates are saved to the correct Trust Stores. For instructions, refer to the [SSL/TLS Certificates for Managed Appliances Guide](#).
- **License Expiration:** Review the [Stealthwatch Smart Software Licensing Guide](#) for details.
- **Removing an Appliance:** If you remove an appliance from Central Management while the configuration channel is down, make sure you also remove the appliance from System Configuration:
  - Log in to the appliance console as sysadmin.
  - Type `SystemConfig`. Press Enter.
  - Select **Recovery > RemoveAppliance**.

Opening Appliance Administration Interface

You can access the Appliance Admin interface through Central Management or by logging in to the appliance directly.

You may need to log in to Appliance Admin if you’ve removed your SMC from Central Manager for troubleshooting.

1. In your browser address bar, type the appliance IP address as follows:

   ```
   https://<IPAddress>
   ```

   - **SMC:** add `/smc/index.html` after the IP address.
   - **Example:** `https://1.1.1.1/smc/index.html`

2. Press Enter.
Replacing the Appliance Identity

Each Stealthwatch version 7.x appliance is installed with a unique, self-signed appliance identity certificate. To replace the appliance identity certificate with a certificate from a Certificate Authority, refer to the SSL/TLS Certificates for Managed Appliances Guide for instructions.

Your certificates are critical for your system’s security. Improperly modifying your certificates can stop Stealthwatch appliance communications and cause data loss.

Changing the Host Name, Domain Name, or IP Address

To change the appliance host name, network domain name, or IP address after you’ve installed and configured your appliances, follow the instructions in the SSL/TLS Certificates for Managed Appliances Guide.

As part of the procedure, you will remove the appliance from Central Management temporarily, and the appliance identity certificate is replaced automatically.

The appliance identity certificate is replaced automatically as part of this procedure.

If your appliance uses a custom certificate, please contact Cisco Stealthwatch Support to change these settings. Do not use the instructions shown here. Make sure you have a copy of the custom certificate and private key.

Opening the Appliance Setup Tool

Use the following instructions to open the Appliance Setup Tool after you’ve configured an appliance.

If you change the host name, network domain name, or IP address using the Appliance Setup Tool, the appliance identity certificate is replaced automatically.

If your appliance uses a custom certificate, please contact Cisco Stealthwatch Support to change these settings. Do not use the instructions shown here. Make sure you have a copy of the custom certificate and private key.
1. In the appliance browser address bar, after the IP address, replace the end of the URL with /lc-ast:

https://<IP_ADDRESS>/lc-ast

2. Press Enter.
3. For more information, refer to 1. Configuring Your Appliances

System Configuration Overview

We’ve updated System Configuration with a new menu structure. System Configuration often involves troubleshooting. For assistance, please contact Cisco Stealthwatch Support.

- **Users:** The available menus are determined by whether you log in as root, sysadmin, or admin.
- **SSH:** You may need to enable SSH to access a menu.

1. Log in to the appliance console.
2. Type **SystemConfig**. Press Enter.
3. From the main menu, select a menu:

- **Network:** To change appliance management port network, trusted hosts, and network interfaces, select Network.
- **Security:** To change or reset passwords and manage Syslog Compliance, select Security.
- **Recovery:** To remove an appliance from Central Management, reset factory defaults, or refresh the image, select Recovery.
- **Advanced:** To refresh the appliance model, open the root shell, manage the admin user account, or configure Single Sign-On, select Advanced.

Changing the Trusted Hosts

You can use System Configuration to change the trusted hosts list from the appliance defaults. However, please contact Cisco Stealthwatch Support before you change your trusted hosts.

⚠️ Please contact Cisco Stealthwatch Support before you change your trusted hosts.
If you change the trusted hosts list from the defaults, make sure each Stealthwatch appliance is included in the trusted host list for every other Stealthwatch appliance in your deployment. Otherwise, the appliances will not be able to communicate with each other.

1. Log in to the appliance console as sysadmin.
2. Select Network > Trusted Hosts.
3. Follow the on-screen prompts to change the Trusted Hosts.

### Resetting Factory Defaults

Use the following instructions to reset an appliance to its factory defaults (RFD). To completely erase data, make sure you reset factory defaults twice.

- **RFD twice**: To completely erase data, make sure you reset factory defaults twice.
- **Back up Configuration**: If you plan to restore the appliance configuration, make sure you save the backup configuration and database backup files. Refer to Backup Configuration Files (in Central Management) and Backup/Restore Database (Appliance Admin interface) topics in the Stealthwatch Online help for details. To restore the backup after RFD, contact Cisco Stealthwatch Support.

If you reset factory defaults (RFD) on an appliance, all existing data and configuration information will be deleted and can only be restored if you’ve made a backup.

If you reset an appliance to factory defaults, you cannot restore the configuration using Central Management. For assistance, please contact Cisco Stealthwatch Support.

1. Log in to the appliance console as sysadmin.
2. Select Recovery > Factory Defaults.
3. Follow the on-screen prompts to reset factory defaults and restart the appliance.

Make sure you RFD each appliance twice to completely erase data.

4. Log in to the appliance console as **sysadmin** and follow the on-screen prompts to configure the appliance IP address, host name, and domain. For instructions, refer to your Stealthwatch hardware or Virtual Edition installation guide. This step is required even if you preserve network settings when you RFD.
5. Log in to the Appliance Setup Tool and add the appliance to Central Management. For details, refer to Adding an Appliance to Central Management.
RFD of a Flow Collector (Special Instructions)

The following instructions only apply to customers that Use NetFlow or NVM telemetry (Distributed Data Store or Centralized Data Store). It does not impact SAL-only customers.

You can opt to RFD a Flow Collector without RFDing the other appliances in your deployment. In v7.3.2, this can result in the newly RFD’d Flow Collector re-using IDs for flow-IDs which are already in the DB (NetFlow, sFlow). This can result in incorrect query results and detections.

To avoid this, you must RFD your Flow Collector by following the steps below:

1. STOP traffic being sent to the Flow Collector.
2. RFD the Flow Collector.
3. Apply the necessary patch for this issue.

Enabling/Disabling Admin Users

Use the following instructions to enable or disable the default admin account.

1. Log in to the appliance console as sysadmin.
2. Select Advanced.
4. Follow the on-screen prompts to enable or disable the Admin User account.
5. Repeat these instructions to enable or disable the Admin User account on all appliances in your Stealthwatch cluster.

Enabling or Disabling Password Reset

Use the following instructions to enable or disable the password reset function. If you select Enable, passwords can be reset to the default settings using the GRUB command line interface.

If you disable the password reset, and you lose your passwords, you will lose access to the data saved to your appliance. To access the appliance again, reset factory defaults and reconfigure it.

1. Log in to the appliance console as root.
2. Type SystemConfig. Press Enter.
4. Select **Password Reset**.
5. Follow the on-screen prompts to enable or disable password reset.

**Resetting Passwords to Default Settings**

There are two ways to reset your passwords to their default settings.

- **Admin Password**: Use [Resetting the Admin Password on the SMC](#).
- **Admin, Root, Sysadmin Passwords**: Use [Resetting Admin, Root, Sysadmin Passwords to Default](#).

> After you reset your appliance passwords to the default, make sure you change them. This step is critical for security. Refer to [Changing Passwords](#) for instructions.

**Resetting the Admin Password on the SMC**

Use the following instructions to reset your **admin** password to the default setting on the SMC. Then, change the appliance password for maximum security.

- **Requirements**: You need the appliance root password to complete these instructions.
- **Other Users**: These instructions reset the admin user to the default password. The individual user passwords will not be changed.
- **Other Appliances**: These instructions do not reset the admin password on other Stealthwatch appliances (Flow Collector, Flow Sensor, or UDP Director).

1. Log in to the appliance console as root.
2. Type `rm /lancope/var/smc/config/users/admin/user.xml`. Press Enter.
3. Type `docker restart smc`. Press Enter.
4. Type `docker restart nginx`. Press Enter.

   This will reset admin password to the default value.

5. Exit the appliance console.
6. Go to **Changing Passwords** to change the admin password from the default. This step is critical for security.

**Resetting Admin, Root, Sysadmin Passwords to Default**

Use console access to reset your appliance **admin**, **root**, and **sysadmin** passwords to the default settings. Then, change the appliance passwords for maximum security.
1. Log in to the appliance console (CIMC or hypervisor).
2. Reboot the appliance.
3. When the console screen reaches the GRUB menu, type "e" to enter edit mode.

4. Advance the cursor to the second line.

   The command line might look slightly different depending on your appliance version.

5. Type `resetpassword` after `c=off` to make the command line look like the following example:
6. Type CTRL-X to resume booting.

This will reset your admin, root, and sysadmin passwords to their default values.

7. Go to Changing Passwords to change the passwords from the default. This step is critical for security.

Changing Passwords

Use the following instructions to change your passwords from the default password or a previous password. Make sure you use the following criteria:

- **Length:** 8 to 256 characters
- **Change:** Make sure the new password is different from the previous password by at least 4 characters.

<table>
<thead>
<tr>
<th>User</th>
<th>Default Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>lan411cope</td>
</tr>
<tr>
<td>root</td>
<td>lan1cope</td>
</tr>
<tr>
<td>sysadmin</td>
<td>lan1cope</td>
</tr>
</tbody>
</table>
Changing the Sysadmin Password

1. Log in to the appliance console as sysadmin.
2. Select **Security**.
3. Select **Password**.
4. Follow the on-screen prompts to change the sysadmin password.
5. Exit System Configuration.

Changing the Root Password

1. Log in to the appliance console as root.
2. Type **SystemConfig**. Press Enter.
3. Select **Security**.
4. Select **Password**.
5. Follow the on-screen prompts to change the root password.

Changing the Admin Password on the SMC

1. Log in to the SMC as admin.
   - **URL**: https://<IPAddress>
   - **Login**: admin
   - **Default Password**: lan411cope

2. Click the **Global Settings** icon. Select **User Management**.
3. Locate the **admin** user in the list.
4. Click the **Actions** menu. Select **Change Password**.
5. Follow the on-screen prompts to change the admin password. Use the following criteria:
   - **Length**: 8 to 256 characters
   - **Change**: Make sure the new password is different from the default password by at least 4 characters.

Changing the Admin Password on All Other Appliances

Use the following instructions to change the admin user password on a Flow Collector, Flow Sensor, or UDP Director.
1. Log in to the Appliance Administration interface as admin.
   - **URL:** https://<IPAddress>
   - **Login:** admin
   - **Default Password:** lan411cope

2. Select Manage Users > Change Password.
3. Enter the current password and new password.
4. Click Apply. Follow the on-screen prompts to change the password.
5. To change the admin password on another appliance, repeat steps 1 through 4.
Installing Patches and Updating Software

Make sure you keep Stealthwatch up-to-date by installing the latest patches for your software version. For details and instructions, visit Cisco Software Central.

Software updates are also posted to your Cisco Smart Account at Cisco Software Central. For a successful update, make sure you follow the instructions in the Stealthwatch Update Guide.
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 email: tac@cisco.com
- For phone support: 1-800-553-2447 (U.S.)
Copyright Information

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)