Stealthwatch® System
Hardware Configuration Guide
(for Stealthwatch System v6.10)
Copyrights and Trademarks

© 2017 Cisco Systems, Inc. All rights reserved.

NOTICE

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.
# CONTENTS

## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Overview</td>
<td>1</td>
</tr>
<tr>
<td>Audience</td>
<td>1</td>
</tr>
<tr>
<td>Stealthwatch Hardware Components</td>
<td>1</td>
</tr>
<tr>
<td>How to Use This Guide</td>
<td>4</td>
</tr>
<tr>
<td>Contacting Support</td>
<td>5</td>
</tr>
<tr>
<td>Configuring a System</td>
<td>7</td>
</tr>
<tr>
<td>Overview</td>
<td>7</td>
</tr>
<tr>
<td>Process Overview</td>
<td>7</td>
</tr>
<tr>
<td>Configuring the Individual Appliances</td>
<td>7</td>
</tr>
<tr>
<td>Configuring the System</td>
<td>13</td>
</tr>
<tr>
<td>Configuring the UDP Director from the SMC</td>
<td>22</td>
</tr>
<tr>
<td>Creating a Management Channel</td>
<td>22</td>
</tr>
<tr>
<td>Adding a UDP Director</td>
<td>23</td>
</tr>
<tr>
<td>Configuring Forward Rules</td>
<td>24</td>
</tr>
<tr>
<td>Configuration through the Appliance Admin Interface</td>
<td>26</td>
</tr>
<tr>
<td>Log in to the Appliance Administration Interface</td>
<td>26</td>
</tr>
<tr>
<td>Configure the System Time</td>
<td>28</td>
</tr>
<tr>
<td>Configure the Flow Sensor</td>
<td>30</td>
</tr>
<tr>
<td>Configure UDP Director Rules</td>
<td>32</td>
</tr>
<tr>
<td>Configure the UDP Director HA</td>
<td>34</td>
</tr>
<tr>
<td>Restart the Appliance</td>
<td>37</td>
</tr>
<tr>
<td>Verifying Communications</td>
<td>39</td>
</tr>
<tr>
<td>Overview</td>
<td>39</td>
</tr>
</tbody>
</table>

© 2017 Cisco Systems, Inc. All Rights Reserved.
Verify NetFlow Data Collection ........................................................................................................39

Adding Cisco ISE ..................................................................................................................................41
  Overview ...........................................................................................................................................41
  Add a Cisco ISE .................................................................................................................................41

Enabling the SLIC Threat Feed Feature .............................................................................................43
INTRODUCTION

Overview

This guide describes and explains how to configure the following Stealthwatch® System hardware:

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

This guide assumes that you have already installed the hardware according to the instructions in the Stealthwatch System Hardware Installation Guide.

For the configuration of the Virtual Edition (VE) products, see the installation and configuration guides of those virtual appliances (SMC VE and Flow Collector VE, the Flow Sensor VE, and the UDP Director VE).

Read this chapter to learn more about this guide and how to contact Support, if needed. This chapter includes the following sections:

- Audience
- Stealthwatch Hardware Components
- Introduction
- How to Use This Guide

Audience

The primary audience for this guide is administrators who need to configure all Stealthwatch physical appliances.

Stealthwatch Hardware Components

The Stealthwatch System is made up of several hardware components that gather, analyze, and present information about your network to improve network performance and security.
This section describes the major Stealthwatch components. The Stealthwatch Management Console (SMC) is the control center for Stealthwatch. It manages, coordinates, configures, and organizes all of the different components of the system. The SMC client software allows you to access the SMC’s user-friendly graphical user interface (GUI) from any local computer with access to a Web browser. Through the client GUI, you can easily access real-time security and network information about critical segments throughout your enterprise.

The SMC:
- Supports up to 25 Stealthwatch Flow Collectors
- Delivers access to a distributed host behavior database
- Supports multiple concurrent users
- Provides a report scheduler to automate periodic reporting
- Provides event forwarding direct to relevant staff and to multiple third party systems
- Supports syslog in association with intelligence gained by Stealthwatch behavioral analysis
- Provides graphical charts for visualizing traffic
- Provides drill-down analysis for troubleshooting
- Provides consolidated and customizable reports
- Immediate notification of security breaches

Flow Collector


The Flow Collector aggregates high-speed network behavior data from multiple networks or network segments to deliver end-to-end protection and improve performance across geographically dispersed networks.

As the Flow Collector receives data, it identifies known or unknown attacks, internal misuse, or misconfigured network devices, regardless of packet encryption or fragmentation. Once Stealthwatch identifies the behavior, the system can take any action you have configured it to take, if any, for that kind of behavior.

The Flow Collector:
- Depending on model up to Flow Collector 4000, processes up to 120,000 flow records per second from up to 1,000,000 hosts
- The Flow Collector 5000 Series processes up to 240,000 flows per second from millions of hosts using over 4000 flow-exporting devices
- Receives flow data from flow exporting devices
- Deduplicates processes and stores bidirectional flows
- Creates and stores host profiles, host pair data, Concern Index™ events, Interface data, Host Group data, VM data and TopN statistics
- Stores domain configuration data
- Forwards alerts to the Stealthwatch Management Console
- Supports up to 5 mitigation devices

**Flow Sensors**

The Stealthwatch Flow Sensor is a network appliance that operates similarly to a traditional packet capture appliance or IDS in that it plugs into a switch port analyzer (SPAN), mirror port, or Ethernet test access port (TAP). The Flow Sensor augments visibility into the following network areas:

- Where flow export is not available.
- Where flow export is available, but you want deeper visibility into performance metrics and packet data.

By directing the Flow Sensor toward any NetFlow v9-capable or IPFIX-capable flow collector you can derive valuable detailed traffic statistics from NetFlow. When combined with the Stealthwatch Flow Collector for NetFlow, the Flow Sensor also provides deep insight into performance metrics and behavioral indicators. These flow performance indicators provide insight into any round-trip latency introduced by the network or by the server-side application.

Because the Flow Sensor has packet-level visibility, it can calculate round-trip time (RTT), server response time (SRT), and packet loss for TCP sessions. It includes all of these additional fields in the NetFlow records that it sends to the Stealthwatch Flow Collector for NetFlow.

**UDP Director**

The UDP Director is a high-speed, high-performance UDP packet replicator. The UDP Director is very helpful in redistributing NetFlow, sFlow, syslog, or Simple Network Management Protocol (SNMP) traps to various collectors. It can receive data from any connectionless UDP application and then retransmit it to multiple destinations, duplicating the data if required.

**Identity Device**

The Stealthwatch System includes the identity device Cisco ISE (Identity Services Engine) including Cisco ISE-PIC. These devices map IP addresses to user names by passively pulling user authentication information from user identity databases. The SMC seamlessly manages multiple identity appliances.
Use the following table to record the settings that you will need to configure Stealthwatch appliances.

<table>
<thead>
<tr>
<th>Settings</th>
<th>SMC</th>
<th>Flow Collector</th>
<th>Flow Sensor</th>
<th>UDP Director</th>
<th>Identity Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td>192.168.1.1</td>
<td>192.168.1.4</td>
<td>192.168.1.7</td>
<td>192.168.1.2</td>
<td>192.168.1.10</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gateway</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Server(s)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NTP Server(s)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mail Relay</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*These are default IP addresses. The Flow Collector sFlow default is 192.168.1.5. The default for the Flow Collector 5000 Series Database is 192.168.1.15.

In addition, you could also use the following settings:

Port exporting flow data (usually 2055) ___________________________

SNMP read-only community string of routers __________________________

How to Use This Guide

In addition to this introduction, we have divided this guide into the following chapters:

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring a System</td>
<td>How to configure appliances to begin processing traffic data</td>
</tr>
<tr>
<td>Verifying Communications</td>
<td>How to establish and verify that the SMC is receiving NetFlow data and how to turn on the SLIC threat feed</td>
</tr>
</tbody>
</table>
### Chapter Description

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adding an Identity Device</td>
<td>How to add an identity device</td>
</tr>
<tr>
<td>Enabling the SLIC Threat Feed Feature</td>
<td>How to enable the SLIC Threat Feed feature in the SMC Client</td>
</tr>
</tbody>
</table>

### Abbreviations

The following abbreviations may appear in this guide:

<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>

### 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
- For phone support: 1-800-553-2447 (U.S.)
CONFIGURING A SYSTEM

Overview
This chapter provides the procedures for configuring the appliance to begin processing traffic data. Once you have completed the steps in this chapter, the installation and configuration process is complete.

Note: Please refer to the checklist on "Introduction" on page 1 for the information you will need before proceeding.

Process Overview
Configuring a Stealthwatch System involves completing the following procedures, which we discuss in this chapter:

1. Configuring the Individual Appliances
2. Configuring the System
3. Configuration through the Appliance Admin Interface

Configuring the Individual Appliances
Initial configuration of every appliance is done with the Appliance Setup Tool. The first time you access the appliance, the Appliance Setup Tool is displayed.

Before you begin, gather the information detailed in the Prerequisite section of “Introduction” on page 1

Note: Your screens may look slightly different from the ones presented here depending on your environment.

To configure an appliance, complete the following steps:

1. In the address field of your browser, type https:// followed by the IP address of the appliance, and then press Enter.
2. The admin login page opens. Type `admin` and `lan411cope` (both are case sensitive), and then click **Login**. Go to step 5.

3. For the SMC, the landing page opens.

To log in, do the following:

a. In the User Name field, type **admin**.

b. In the Password field, type **lan411cope**.

c. Click **Sign in**.

5. The Welcome page opens. Click **Continue**.
The Management Network Interface page opens.

6. Enter the IP addresses for the appliance, and then click **Next**. The Password Management page opens.
7. In the appropriate fields, type your new admin password, and then click **Next**. The Host Name and Domain page opens.

8. In the appropriate fields, type the host name and the network domain name, and then click **Next**. The DNS Settings page opens.
9. Click the + button, and then type the IP address of the DNS server. Click **Next**. The NTP Settings page opens.

**Note:** Please set the first NTP server to be pool.ntp.org. This will allow the Stealthwatch appliance to access the random ntp.org pool of NTP servers to set the appliance’s time.
10. You can accept the default setting or enter another server by entering the IP address of your NTP server or selecting a name by clicking the list icon and selecting one from the drop-down list. See Configuration through the Appliance Admin Interface.

11. Click **Next**. The Review page opens.

12. Review your settings, and then click **Apply**. The confirmation dialogue opens.

13. Allow a few minutes for your new system settings to take effect and then click **Next**. When finished, the login page for the appliance opens.

14. Enter the login credentials, and then click **Login**.

15. Do you have any other appliances to configure?
   - If yes, return to Step 1 and repeat this procedure for the next appliance. Remember to configure the primary SMC last.
   - If no, go to the next step.
16. After configuring the last or only SMC, continue with the next section, Configuring the System.

**Configuring the System**

After you finish configuring all appliances including the SMC (VE), you can configure the system.

**CAUTION!** All appliances managed by the SMC must be activated. Otherwise, the SMC cannot communicate with the Flow Collector and the system cannot be configured properly.

**Important:** If you are configuring a failover SMC, you need to supply only the Domain Name for its system, and then click Next for the remaining pages. You can then set up your system when you configure it for the primary SMC.

The Welcome page of the System Setup Tool opens.

1. Click **Continue**. The Add Enterprise Domain Information page opens.
2. Enter the range of IP addresses for your system (you can use CIDR, dashed-ranges, trailing dot subnet, or IPv6) or Bulk Upload to import a CSV file of IP addresses ranges, and then click Next. The Appliance page opens.

**Note:** The IP addresses in the CSV file must be separated by one of following: comma, comma space, space, space, return.
3. Click the + button. The Add Flow Collector dialog opens.

4. Enter the Flow Collector IP address, and then click **Next**. The Communication dialogue opens:

   **Conditional procedure:** When adding a Flow Collector or Flow Sensor in this step, you must have first created a management channel between the Flow Collector or Flow Sensor and the Stealthwatch Management Console (SMC). If you have not done this, you will receive an error message at this point in the procedure. To create the management channel for each Flow Collector and Flow Sensor, complete the following steps:

   1. Log in to the applicable Appliance Admin interface using your browser and the IP address of the appliance.
   2. In the left navigation pane, click **Configuration > Management Systems Configuration.**
   3. Click **Add New Management System.**
   4. In the Management System IP Address field, type the SMC's IP address.
   5. Select the **Is SMC** check box.
   6. Click **Apply.**
   7. In the Error dialog in the System Setup Tool, click **Cancel,** and then click **Apply.**
5. Click **Add**. The Flow Collector (is added to the system:

![Flow Collector Added]

6. Click **Next**. The Appliance Flow Sensors page opens.

![Appliance Flow Sensors Page]

7. Do you have Flow Sensors to add?
   - If yes, click the + button and go step 9.
   - If no, click **Next** and go to the next step.

8. The warning message displays. Click **OK**. Go to step 14.

![Warning Message]

9. Click the + button. The Add Flow Sensor dialogue appears:

![Add Flow Sensors](image)

10. Type an IP Address, and then click OK. The Communication Established dialogue appears.

![Communication Established](image)

11. From the drop-down list select a Flow Collector, and then click Add.

![Flow Sensor VE Login Credentials](image)

The Flow Sensor is added.
12. Click **Next**. The SMTP Setting page opens:

13. Enter the email address that you want in the “from” field when the SMC sends emails.

14. Enter the SMTP Relay address, and then click **Next**. The SNMP page opens:
15. If necessary, modify the settings (only one string can be set here), and then click **Next**.

**Note:** If you select SNMP Version 3, then you must enter a user name, and then can select as options, authentication and encryption.

16. The Internet Access (for the SMC) page opens.
17. Select the proper type of Internet access:

- **No access**: Your SMC is not connected to the Internet. You will have to gain access to acquire a license from the Download and Licensing Center. Click **Next** on the Offline page to open the Complete page.

- **Access via Proxy Server**: Your SMC is connected to the Internet through a proxy server. The proxy settings appear.

Complete the settings for your proxy server, and then click **Next**.

20. If you selected Direct Access or completed the Proxy settings, the Licensing page opens:
21. Click the Download and License Center link. Obtain the license as described in the *Downloading and Licensing Stealthwatch Products* document.

22. After obtaining the license, click **Activate**.

   **Note:** A message will display if an appliance is not registered.

23. Click **OK**. The Complete page opens.
24. Click **Launch** to go to the SMC client landing page. A message opens. If you have not licensed the appliance then you will get a message with information about what has not been licensed. An example message is below:

![Notice](image.png)

25. From the Welcome Admin User drop-down list in the upper right corner, click **Administer Appliance** to open the Appliance Admin interface and continue with the next section, “Configuration through the Appliance Admin Interface” on page 26.

26. Do you have a UDP Director?
   - If yes, continue with the next section, Configuring the UDP Director from the SMC.
   - If no, continue to the section, Configuration through the Appliance Admin Interface

### Configuring the UDP Director from the SMC

If you have UDP Directors in your Stealthwatch System, you can configure them from the SMC Web Client so that the SMC manages the UDP Directors. In this configuration, the forwarding rules are configured on the SMC.

To manage the UDP Director individually (as a standalone appliance), see Configuring a System

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

### Creating a Management Channel

Before the UDP Director can be added to the SMC, you must create a management channel between the two appliances.

1. Log in to the UDP Director Appliance Admin interface using your browser and the IP address of the appliance.
2. In the left navigation pane, click **Configuration > Management Systems Configuration**.
3. Click **Add New Management System**.
4. In the Management System IP Address field, type the SMC’s IP address.
5. Select the **Is SMC** check box.
6. Click **Apply**.

**Adding a UDP Director**

To add a UDP Director to the SMC, complete the following steps:

1. Log in to the SMC Web App.
2. From the navigation menu, click the user name at the top right of the page, and click **UDP Director Configuration**.
3. Click **Add New Configuration**.
4. Type in a name and the IP address of the UDP Director.
5. Click Save.
6. If you have additional UDP Directors, repeat steps 2-5 for each one.
7. Continue to the next section, Configuring Forward Rules

Configuring Forward Rules

After adding a UDP Director to the SMC, you can configure forward rules for it.

To configure forwarding rules for a UDP Director, complete the following steps:


2. Click Add New Rule.
3. In the Description field, enter a brief description that identifies the rule.
4. In the Source IP Address:Port List field, type the IP address of the device that sends data to the UDP Director followed by the port number through which the data will be sent.

Notes:
- Use the syntax [IP address]:[Port Number], as shown in the examples below.
- You can use Classless Inter-Domain Routing (CIDR) notation to enter a range of IP addresses.
- You can type "All" to accept data from any source IP address on this port.
- 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

5. In the Destination IP Address field, enter the IP address of the device receiving data from the UDP Director.
6. In the Destination Port Number field, enter the port number for the receiving device.
7. Click **Save**. The new rule is added to the table on Forwarding Rules page.
8. Do you want to sync the changes?
   a. If yes, click the Sync button at the top of the page. The new rule is saved.
   b. If no, click the Discard Edits button at the top of the page. When the Configuration dialogue appears, click **Yes**.
9. Repeat the procedure to add forwarding rules as needed.
10. Continue with the next section, **Configuration through the Appliance Admin Interface**.

**Note:** If you want to have a secondary UDP Director, you must have added it with at least one forwarding rule. You first need to configure the Primary UDP Director and then repeat the configuration on the Secondary one. For the instructions for configuring HA appliances, go to Configure the Primary UDP Director HA.

## Configuration through the Appliance Admin Interface

This section provides the following procedures to complete the configuration of a virtual appliance using its Appliance Admin interface:

1. **Log in to the Appliance Administration Interface**
2. **Configure the System Time**
3. **Configure the Flow Sensor**
4. **Configure the UDP Director HA**
5. **Restart the Appliance**

### Log in to the Appliance Administration Interface

To log in to the Appliance Administration (Admin) interface, complete the following steps:

**Notes:**

- The supported browsers for Stealthwatch are Internet Explorer version 11 and later, and the latest versions of Firefox, Google Chrome, and Safari.
- If you have trouble loading any of the pages, try a different browser, or clear your browser cache, close and re-open your browser, and then log in again.

1. In the address field of your browser, type `https://` followed by the IP address of the appliance, and then press **Enter**.
Note: Depending on the speed of your VM host, it may take approximately 30 minutes for all services to boot up.

2. Are you opening the SMC Appliance Admin interface?
   - If yes, the Landing page opens. In the upper right corner, click the Settings icon, and then click **Administer Appliance**.
   - If no, the virtual appliance Login page opens.

3. In the **User Name** field, type **admin**.
4. In the **Password** field, type the admin password you created in the appliance setup.
5. Click **Login**. The Appliance Admin interface Home page opens.
6. Continue with the next section, “Configure the System Time.”

Configure the System Time

To configure the Network Time Protocol (NTP) and system time (time zone) settings on the appliance, complete the following steps:

**CAUTION!** Use the same NTP server used for the Flow Collectors and other devices that feed information to the SMC. If you have a Flow Collector 5000 Series appliance, configure the NTP and system time settings in the database and the engine so they are the same.

1. On the Appliance Admin interface navigation pane, click the plus sign (+) beside Configuration and then click System Time and NTP.

The NTP Server page opens showing the NTP server that you set in the initial configuration using the Appliance Setup Tool.
2. Scroll down to the Time Zone section of the page to configure the appliance system time.

3. Do the following:
   - Select the Continent from the drop-down list.
   - Select the Country from the drop-down list.
   - Select the Timezone from the drop-down list.
   The Apply notice appears.
4. Click **Apply** to make the changes permanent. The confirmation window opens.

![Confirmation Window](image)

5. Click **OK**.

6. Are you configuring a Flow Sensor or a UDP Director?

   - If you are configuring a Flow Sensor, continue with the next section, Configure the Flow Sensor.
   - If you are configuring a UDP Director, continue with the section, Configure UDP Director Rules.
   - If no, continue to the section, Restart the Appliance.

### Configure the Flow Sensor

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

To configure how the Flow Sensor exports application identification and payload data, complete the following steps:

1. In the navigation page, click the plus sign beside Configuration menu, and then click **Advanced Settings**.

![Navigation Page](image)
The Export settings page opens.

2. 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>Export HTTPS Header Data</td>
<td>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>Export HTTP Header Data</td>
<td>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>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</td>
</tr>
</tbody>
</table>
### Item | Description
--- | ---
 | requires that the Flow Type is set to IPFIX.
Flow Export Format | Allows you to specify whether the Flow Sensor uses IPFIX or NetFlow v9 to send flow data to the collector.

| 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.
 | • Use only when the Flow Sensor has only two ports and is connected by a TAP.
 | **Use independent caches for each monitoring port**
 | • Allows deduplication of packets across each Flow Sensor interface.
 | • Uses more memory.
 | • Higher overall pps processing rates.
 | • Each interface maintains its own latency and application database.
 | • Results in a unique NetFlow record for each interface that sees a given packet.

3. Click **Apply** to save your settings.
4. Continue with the section, “Restart the Appliance” on page 37.

### Configure UDP Director Rules

If you are not managing the UDP Director from the SMC, you can configure the forwarding rules on the appliance Admin page. For the UDP Director, you need to configure the exporter to send flows to be forwarded to the IP address of eth0. The UDP Director will then forward these from eth0 while preserving the original IP and MAC address of each exporter for forwarded packets.

**Note:** For promiscuous reception, you should use a span filter for all traffic of interest. The network must allow traffic on the ports being used from the exporters to the UDP Director and then to the receivers (ACLs).

To configure the rules for the UDP Director, complete the following steps:
1. In the navigation pane, click the plus sign (+) beside **Configuration** and then click **Forwarding Rules**.

The Forwarding Rules page opens.

2. In the Description field, type a description of the rule.

3. In the Source IP Address:Port List field, type the IP address of the device that sends data to the UDP Director followed by the port number through which the data will be sent. Use the following syntax:

   \[[IP \text{ address}]:[\text{Port Number}]\text{ as in }10.201.1.41:2057\]

   **Note:**
   - To receive all traffic from any device from a specific port, type \text{All}:[\text{port number}]. For example, type \text{All:3123}
You can also use CIDR (Classless Inter-Domain Routing) notation to enter a range of IP addresses. For example, type **172.200.1.0/16:9000**

**Tip:**
- Use "All", or CIDR ranges where possible for the inputs to limit the amount of parsing required by the engine. Using many individual IP addresses for the input causes the engine to work harder.
- Also, you can use substitute ports for the input traffic and then redirect that traffic to the desired output ports. For example, rather than sending all port 55431 traffic to one rule, you can break up that traffic by having 1/3 of the exporters that formerly used port 55431 to use a dummy port of 44440 instead. Then you can have 1/3 of the exporters use port 44441, and 1/3 of the exporters use port 44442. Then redirect all that traffic for ports 44440, 44441, and 44442 to the single destination port of 55431.

4. To add another entry, press **Enter** and type the next IP address and port number.
5. In the Destination IP Address field, type the IP address of the device that receives data from the UDP Director.
6. In the Destination Port Number field, type the port number for the receiving device.
7. If you have more than one device sending data to the UDP Director to be forwarded to another receiving device, click **Add**.

   A new line appears where you can enter the settings. Repeat this step until you have entered all devices for this UDP Director.

8. When finished, click **Apply**. The UDP Director Configuration screen refreshes and the system updates the configuration file. Any errors appear at the top of the screen.
9. Are you configuring a UDP Director HA?
   - If yes, continue to the next section, **Configure the UDP Director HA**.
   - If no, continue with the section, “Restart the Appliance” on page 37.

**Configure the UDP Director HA**

The UDP Director High Availability allows a user to configure settings for redundant UDP Director 2000s. Both nodes are fully redundant, however only one node is online at a time. 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.

**Important:** You must have at least one rule for the UDP Director in the HA system. If the UDP Director has already been configured with rules, it is recommended to export (save...
You first need to configure the Primary UDP Director and then repeat the configuration on the Secondary one. If the both UDP Directors are new, then you must follow the procedures for each in this Guide. However, if the secondary is already configured as an appliance on the Stealthwatch System, then you would simply need to log in to the secondary UDP Director and configure its HA components as described here.

**Configure the Primary UDP Director HA**

To configure the primary UDP Director:

1. In the navigation pane of the UDP Director Admin interface, click the plus sign (+) beside Configuration, and then click **High Availability**.

2. On the Enable High Availability Cluster page, select the Enable High Availability check box for the High Availability Settings.
3. In the Virtual IP Address and the Subnet Mask fields, type the IP addresses for the primary UDP Director. (They are the same for the secondary.)

**Note:** The Virtual IP Address should be in the same subnet as the unicast addresses.

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

5. 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.)

6. In the fields for Sync Ring 2 (Eth3) Unicast IP Address, enter the IP address and the subnet mask.

**Note:** Each of the IP addresses—eth0, eth02, eth03—must be on its own separate unicast subnet.

7. After reviewing the setting, click **Apply** to set the configuration.

8. Continue to the next section to configure the second UDP Director of the cluster.

**Configure the Secondary UDP Director HA**

To configure the secondary UDP Director complete the following steps:

1. Log in to the Appliance Admin interface for the secondary UDP Director 2000 of the HA pair.

2. 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.

3. Click Apply to save your changes and to start the clustering services on this appliance.
4. Click the Promote button to designate the appliance that is the primary one.
5. Continue to the next section.

Restart the Appliance

To restart the appliance, complete the following steps:


   ![Restart Appliance interface](image)

   The confirmation dialog opens.

   ![Confirmation dialog](image)

2. Click Yes.
3. Did you configure a Flow Collector?
If yes, continue to the next chapter, “Verifying Communications.”
If no, go to the next step.

6. Did you configure a Flow Sensor or UDP Director?
   If yes, congratulations, you have now completely installed and configured the appliance! After you restart the Flow Sensor, it will begin collecting data from the VM environment and sending it to the NetFlow collector. After you restart the UDP Director, it will begin collecting data and sending it to the configured destinations.
   If no, go to the next step.

7. Do you have an Identity device?
   If yes, go to the next chapter, “Adding an Identity Device.”
   If no, go to the next step.

8. Do you have the SLIC feature?
   If yes, go to the chapter, "Enabling the SLIC Threat Feed Feature."
   If no, congratulations, you have completed the configuration of your SMC. After restarting, it will begin communicating with the Flow Collectors.
VERIFYING COMMUNICATIONS

Overview

After you license the Stealthwatch appliances, you must verify that you are receiving NetFlow data. To verify, complete the following procedure as detailed in this chapter:

**CAUTION!** Wait 30 minutes after completing all of the licensing procedures in the previous section for each of the appliances before beginning the procedures in this section.

Verify NetFlow Data Collection

After adding the Flow Collector to the SMC, the Flow Collector will communicate flow information to the SMC, which will display this information in a user-friendly way through various documents. To confirm that you are indeed collecting NetFlow data, complete the following steps:

1. In the Enterprise tree, right-click the Flow Collector and select Status > NetFlow Collection Status.

The NetFlow Collection Status document opens.
2. Look at the **Current NetFlow Traffic** field located at the top of the document. This statistic shows the amount of NetFlow traffic being observed. Are you seeing any flow traffic?

- If yes, go to the next step.
- If no, check your exporter/router configurations. *(For assistance see the SMC Client Online Help.)* Then, go to the next step.

3. Look at the **Longest Duration Export** column. You may need to add this column by right-clicking a column heading and selecting **Longest Duration Export** from the pop-up menu. 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 assistance see the SMC Client Online Help.)*

4. Do you have an Identity device?

- If yes, go to the next chapter, "Adding Cisco ISE."
- If no, go to the next step.

5. Do you have the SLIC feature?

- If yes, go to the chapter, "Enabling the SLIC Threat Feed Feature."
- If no, congratulations, you have completed the configuration of your appliances.
ADDING CISCO ISE

Overview

If you have identity devices, you can add them to the SMC. This chapter includes the procedure for adding the Cisco ISE (Identity Services Engine).

Add a Cisco ISE

Notes:

- You can add multiple independent Cisco ISE clusters to a domain.
- The procedure for adding a Cisco ISE-PIC to your Stealthwatch System is the same as described here. Refer to your Cisco ISE documentation for further information on setting up Cisco ISE-PIC.

To add the Cisco ISE, complete the following steps:

1. On the menu of the SMC Web App interface, select Deploy > Cisco ISE Configuration.

The Add Cisco ISE dialog opens.
2. Type a name for the Cisco ISE cluster. You must configure a Cisco ISE cluster for each Stealthwatch System domain in which it is used.

3. Select the applicable certificate. This is the same name that is entered in the Friendly Name field on the SSL Certificate page (in the "Upload an Identity" section) in the Appliance Administration (Admin) interface that enables the appliance to authenticate its identity as a client (i.e., it is the client certificate that the SMC presents to ISE).

4. Type the IP address of the primary pxGrid node on the ISE cluster with which the appliance is integrating.

5. (Optional) Type the IP address of the secondary pxGrid node on the ISE cluster with which the appliance is integrating. This node is used for failover purposes. If the connection to the primary node fails, the secondary node is used.

6. Type the user name you have configured for your user account on the Cisco ISE device. This name displays in the pxGrid client list on the ISE cluster in the ISE appliance.

7. Click Add > OK. The Cisco ISE is added to the domain in the Identity Services folder.

8. Do you have the SLIC feature?
   - If yes, continue to the next chapter, Enabling the SLIC Threat Feed Feature.
   - If no, congratulations, you have completed the configuration of your appliances.
ENABLING THE SLIC THREAT FEED FEATURE

The last step in installing and configuring the Stealthwatch package is to enable the SLIC Threat Feed through the SMC client interface.

Complete the following steps:

1. In the Enterprise tree, right-click the Stealthwatch Labs Intelligence Center branch and select Configuration > SLIC Threat Feed Configuration.

The SLIC Threat Feed Configuration dialog opens.
2. Select the “Enable the SLIC Threat Feed” checkbox.
3. In the SLIC Feed Key field, type your key.
4. Click OK. Within 10 minutes, the Enterprise tree updates the Command & Control Servers (C&C) host group branch to display the list of active C&C servers identified thus far.

Congratulations! You can now begin enjoying the many security and networking monitoring benefits of the Stealthwatch System. For further assistance, refer to the Stealthwatch Management Console User’s Guide or the SMC client interface online Help. Click Help.