Stealthwatch® Management Console VE and Flow Collector™ VE
Installation and Configuration Guide
(for Stealthwatch System v6.9.0)
# CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contents</td>
<td>iii</td>
</tr>
<tr>
<td><strong>Introduction</strong></td>
<td>1</td>
</tr>
<tr>
<td>Overview</td>
<td>1</td>
</tr>
<tr>
<td>Audience</td>
<td>1</td>
</tr>
<tr>
<td>About the Flow Collector VE</td>
<td>1</td>
</tr>
<tr>
<td>About the SMC VE</td>
<td>2</td>
</tr>
<tr>
<td>Before You Begin</td>
<td>3</td>
</tr>
<tr>
<td>Data Storage</td>
<td>5</td>
</tr>
<tr>
<td>How to Use This Guide</td>
<td>6</td>
</tr>
<tr>
<td>Other Resources</td>
<td>7</td>
</tr>
<tr>
<td><strong>Installing a Virtual Appliance</strong></td>
<td>9</td>
</tr>
<tr>
<td>Overview</td>
<td>9</td>
</tr>
<tr>
<td>Process Overview</td>
<td>9</td>
</tr>
<tr>
<td>Configuring Your Firewall for Communications</td>
<td>10</td>
</tr>
<tr>
<td>Communication Ports</td>
<td>10</td>
</tr>
<tr>
<td>Logging in to the VMware vSphere Client</td>
<td>13</td>
</tr>
<tr>
<td>Adding a Resource Pool</td>
<td>14</td>
</tr>
<tr>
<td>Installing the Virtual Appliance</td>
<td>16</td>
</tr>
<tr>
<td><strong>Configuring the Virtual Environment</strong></td>
<td>25</td>
</tr>
<tr>
<td>Overview</td>
<td>25</td>
</tr>
<tr>
<td>Configure the IP Addresses</td>
<td>25</td>
</tr>
<tr>
<td>Change the Default User Passwords</td>
<td>29</td>
</tr>
<tr>
<td>Changing the sysadmin Password</td>
<td>29</td>
</tr>
<tr>
<td>Changing the root Password</td>
<td>32</td>
</tr>
<tr>
<td><strong>Configuring a System</strong></td>
<td>35</td>
</tr>
</tbody>
</table>

© 2017 Cisco Systems, Inc. All Rights Reserved.
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>35</td>
</tr>
<tr>
<td>Process Overview</td>
<td>35</td>
</tr>
<tr>
<td>Configuring the Individual Appliances</td>
<td>35</td>
</tr>
<tr>
<td>Configuring the System</td>
<td>41</td>
</tr>
<tr>
<td>Expand SMC VE or Flow Collector VE Disk Space</td>
<td>51</td>
</tr>
<tr>
<td>Increasing Memory for the Flow Collector VE</td>
<td>57</td>
</tr>
<tr>
<td>Configuration through the Appliance Admin Interface</td>
<td>59</td>
</tr>
<tr>
<td>Log in to the Appliance Administration Interface</td>
<td>59</td>
</tr>
<tr>
<td>Configure the System Time</td>
<td>61</td>
</tr>
<tr>
<td>Restart the Virtual Appliance</td>
<td>62</td>
</tr>
<tr>
<td><strong>Verifying Communications</strong></td>
<td>65</td>
</tr>
<tr>
<td>Overview</td>
<td>65</td>
</tr>
<tr>
<td>Verify NetFlow Data Collection</td>
<td>65</td>
</tr>
<tr>
<td><strong>Adding Cisco ISE</strong></td>
<td>67</td>
</tr>
<tr>
<td>Overview</td>
<td>67</td>
</tr>
<tr>
<td>Add a Cisco ISE</td>
<td>67</td>
</tr>
<tr>
<td><strong>Enabling the SLIC Threat Feed Feature</strong></td>
<td>69</td>
</tr>
</tbody>
</table>
INTRODUCTION

Overview

This is an installation and configuration guide for the Stealthwatch Management Console (SMC) VE (Virtual Edition) and Flow Collector VE in a network using vSphere Client v4.x or later.

Note: Stealthwatch VE appliances that are running under VMware ESX v3.x are not compatible with ESX v4.x. If you upgrade VMware to ESX v4.x, you must delete your existing Stealthwatch VE appliances and reinstall them.

For Stealthwatch System physical appliances, see the Stealthwatch System Hardware Installation Guide and the Stealthwatch System Hardware Configuration Guide.

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

- Audience
- About the Flow Collector VE
- About the SMC VE
- Before You Begin
- How to Use This Guide
- Resource Requirements

Audience

The primary audience for this guide is administrators who need to install and configure Stealthwatch SMC VE and Flow Collector VE appliances. This guide assumes the audience has a basic familiarity with VMware software.

About the Flow Collector VE

At the heart of the Stealthwatch System is the highly scalable Stealthwatch Flow Collector. The Flow Collector is available as either a physical or a virtual appliance. The Flow Collector VE performs the same functions as its physical counterpart, but in a VMware environment. The Stealthwatch Flow Collector for NetFlow gathers NetFlow, cFlow, J-Flow, Packeteer 2, NetStream, and IPFIX data. To achieve full network visibility with a traditional probe-based
approach, you would need to install a probe for each router or switch on your network. This results in many costly hardware installations. Conversely, Stealthwatch’s flow-based approach provides you with full network visibility at a fraction of the cost. Each Flow Collector can process data for as many as 1,000,000 hosts from up to 2,000 flow exporters, depending on the Flow Collector model and license restrictions.

Using flow-based anomaly detection, the Flow Collector zooms in on any unusual behavior and immediately sends an alarm to the SMC with the contextual intelligence that allows personnel to take quick, decisive action to mitigate any damage. The Flow Collector:

- Gathers data from various flow sources (routers/exporters, switches, firewalls, and Stealthwatch Flow Sensors)
- Analyzes the data gathered
- Creates a profile of normal network activity
- Generates an alert for any behavior that falls outside of the normal profile

**About the SMC VE**

As the control center for the Stealthwatch System, the SMC 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 from any local computer with access to a Web browser. Through the client interface, you can easily access real-time security and network information about critical segments throughout your enterprise.

Also available as a physical or virtual appliance, the SMC enables:

- Centralized management, configuration, and reporting for up to 25 Flow Collectors
- Graphical charts for visualizing traffic
- Drill-down analysis for troubleshooting
- Consolidated and customizable reports
- Trend analysis
- Performance monitoring
- Immediate notification of security breaches

The SMC provides the single vantage point for disparate IT groups to see contextual information about all activity across the network and to investigate accordingly. With the SMC, gone are the days when different IT departments spent hours and even days trying to isolate the root cause of an issue - often blaming each other – before finally being able to deploy the appropriate personnel to take corrective action.

By simply glancing at the SMC’s user-friendly graphical interface, operators can immediately spot and zoom in on any unusual behavior. Using the SMC’s unique drill-down features, administrators can go from identifying the issue to isolating the root cause within minutes, identifying affected applications and users along the way, enhancing operational efficiency and decreasing costs.
In addition, the flexible SOAP-compliant Web application program interface (API) provides ready, programmable access to Stealthwatch data from within enterprise applications, such as Security Incident and Event Managers (SIEMs), network managers, trouble-ticketing systems, and third-party reporting systems.

**Before You Begin**

Use the information in this section to prepare for installing and configuring the Stealthwatch VE appliances. Note that the configuration is a two-part process using first the vSphere client interface, and then the Appliance Administration (Admin) interface. You can use the tables provided in this section to record settings you will need to install and configure the Stealthwatch VE appliances.

You need to install and configure your virtual appliances in the following order:

1. Endpoint Concentrator
2. UDP Director VE
3. Flow Sensor VE
4. Flow Collector VE
5. SMC VE

If you do not follow this recommended order when you set up the Stealthwatch system, the Stealthwatch System may not properly collect data from the appliances and you will have to set up each one separately.

**CAUTION!** Be sure the time setting on the ESX server where you will be installing the virtual appliances reflect the correct time. Otherwise, the appliances may not be able to boot up.

**Downloading the VE Software**

Before you can complete the procedures in this guide, you must obtain the OVF (Open Virtualization Format) file from the Download and Licensing Center. For instructions on downloading the file for each appliance, see the *Downloading and Licensing Stealthwatch Products* document in the Download and Licensing Center or in the Documentation Library found in Help of the Stealthwatch appliances.

**Resource Requirements**

**SMC VE**

To determine the minimum resource allocations for the SMC VE, you should determine the number of Flow Collectors and users expected to log in to the SMC.
Refer to the following specifications to determine your resource allocations:

<table>
<thead>
<tr>
<th>Flow Collectors</th>
<th>Concurrent Users*</th>
<th>Minimum Reserved Memory</th>
<th>Recommended Reserved Memory</th>
<th>Reserved CPUs</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>16 GB</td>
<td>24 GB</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>5</td>
<td>24 GB</td>
<td>32 GB</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>10</td>
<td>32 GB</td>
<td>32 GB</td>
<td>4</td>
</tr>
</tbody>
</table>

*Concurrent users include scheduled reports and people using the SMC client at the same time.

**Reserved Memory**: If your system will have a limited number of Flow Collectors and a small amount of data collection, you can use the Minimum Reserved Memory amount. If your system will have a large amount of data collection, use the Recommended Reserved Memory amount.

**SMC VE 2000**

The following specifications are the default settings for the download of the SMC VE 2000, the minimum recommended, and an estimate of the hardware equivalent:

<table>
<thead>
<tr>
<th></th>
<th>OVF</th>
<th>Minimum Recommended</th>
<th>Hardware Equivalent*</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAM</td>
<td>64 GB</td>
<td>64 GB</td>
<td>128 GB</td>
</tr>
<tr>
<td>CPU</td>
<td>8</td>
<td>8</td>
<td>28</td>
</tr>
<tr>
<td>Storage</td>
<td>50 GB</td>
<td>200 GB</td>
<td>3.6 TB</td>
</tr>
</tbody>
</table>

*These figures are based on the SMC 2010 appliance and physical (non hyper-threaded) cores.

**Flow Collector VE**

To determine your resource allocations for the Flow Collector VE, you should determine the flows per second expected on the network, and the number of exporters and hosts it is expected to monitor. Refer to the following specifications to determine your resource allocations:

<table>
<thead>
<tr>
<th>Flows per second</th>
<th>Exporters</th>
<th>Hosts</th>
<th>Recommended Reserved Memory</th>
<th>Reserved CPUs</th>
<th>Flow Collector VE Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up to 4,500</td>
<td>Up to 250</td>
<td>Up to 125,000</td>
<td>16 GB</td>
<td>2</td>
<td>FCVE</td>
</tr>
<tr>
<td>Up to 15,000</td>
<td>Up to 500</td>
<td>Up to 250,000</td>
<td>24 GB</td>
<td>3</td>
<td>FCVE</td>
</tr>
<tr>
<td>Up to 22,500</td>
<td>Up to 1000</td>
<td>Up to 500,000</td>
<td>32 GB</td>
<td>4</td>
<td>FCVE</td>
</tr>
<tr>
<td>Flows per second</td>
<td>Exporters</td>
<td>Hosts</td>
<td>Recommended Reserved Memory</td>
<td>Reserved CPUs</td>
<td>Flow Collector VE Model</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------</td>
<td>-------</td>
<td>-------------------------------</td>
<td>---------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>Up to 30,000</td>
<td>Up to 1000</td>
<td>Up to 500,000</td>
<td>32 GB</td>
<td>5</td>
<td>FCVE</td>
</tr>
<tr>
<td>Up to 60,000</td>
<td>Up to 1500</td>
<td>Up to 750,000</td>
<td>64 GB</td>
<td>6</td>
<td>2000</td>
</tr>
<tr>
<td>Up to 120,000</td>
<td>Up to 2000</td>
<td>Up to 1,000,000</td>
<td>128 GB</td>
<td>7</td>
<td>4000</td>
</tr>
</tbody>
</table>

These are the Flow Collector VE models and their capacities*:

<table>
<thead>
<tr>
<th>FC VE Model</th>
<th>Flows per second</th>
<th>Exporters</th>
<th>Hosts</th>
<th>Reserved Memory</th>
<th>Reserved CPUs</th>
<th>Maximum Disk Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000</td>
<td>Up to 30,000</td>
<td>Up to 1,000</td>
<td>Up to 500,000</td>
<td>32 GB</td>
<td>5</td>
<td>1 TB</td>
</tr>
<tr>
<td>2000</td>
<td>Up to 60,000</td>
<td>Up to 1,500</td>
<td>Up to 750,000</td>
<td>64 GB</td>
<td>6</td>
<td>2 TB</td>
</tr>
<tr>
<td>4000</td>
<td>Up to 120,500</td>
<td>Up to 2,000</td>
<td>Up to 1,000,000</td>
<td>128 GB</td>
<td>7</td>
<td>4 TB</td>
</tr>
</tbody>
</table>

*These figures are based on tests with VMWare ESXi 5.5.0 892794:

Local and Remote: Dell R620, 384 GB DDR3, 2x es02660 2.2 Hz 8C (16C total), 6x 300 GB, 10K RAID 6, 2x 256 GB Samsug 840Pro VM c/Cache

Local: Dell R720, 128GB DDR3, 2xE5-2670 2.6 GHz8C (16C total), 12x 600 GB 10K RAID 6

NetApp FAS3220 Storage ISCSI/Nfs for the remote file system via 1G links from VMware

**Data Storage**

The maximum amount of data storage allowed on either the Flow Collector VE or the SMC VE is 4 TB. The maximum disk space is 5.6 TB. The virtual appliance uses approximately 75% of the disk for data storage, leaving 25% for the operating system and cache. Therefore, always expand the disk to 40% more than the desired disk amount.

**Important:** Cisco recommends allocating a minimum of 1 GB of disk storage for each day every 1,000 flows per second (FPS) your system averages daily multiplied by the number of days you want to store the flows. For example, If your system averages 2,000 FPS and you want to store flows for 30 days, allocate a minimum of 60 GB (2 X 30) of disk storage space.
Note: If the External Event processing (syslog) feature is used, then more memory and processing resources will be required.

Information Needed for the vSphere Client Interface

<table>
<thead>
<tr>
<th>Setting</th>
<th>ESX/vSphere Server</th>
<th>Flow Collector VE</th>
<th>SMC VE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login User Name</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Login Password</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td>(Default = 192.168.1.4)</td>
<td></td>
<td>(Default = 192.168.1.11)</td>
</tr>
<tr>
<td>Netmask IP Address</td>
<td>(Default = 255.255.255.0)</td>
<td></td>
<td>(Default = 255.255.255.0)</td>
</tr>
<tr>
<td>Gateway IP Address</td>
<td>(Default = 192.168.1.1)</td>
<td></td>
<td>(Default = 192.168.1.1)</td>
</tr>
</tbody>
</table>

Information Needed for the Appliance Admin Interface

<table>
<thead>
<tr>
<th>Setting</th>
<th>Flow Collector VE</th>
<th>SMC VE</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>(Default = 192.168.1.4)</td>
<td>(Default = 192.168.1.11)</td>
</tr>
<tr>
<td>Host Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Domain Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NTP Server IP Address(es)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS Server IP Address(es)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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>2. &quot;Installing a Virtual Appliance.&quot;</td>
<td>How to configure your firewall for communications, add a resource pool, and install the software</td>
</tr>
<tr>
<td>3. Configuring the Virtual Environment</td>
<td>How to set up the virtual environment for the appliances</td>
</tr>
<tr>
<td>4. Configuring a System</td>
<td>How to configure appliances to begin processing traffic data</td>
</tr>
</tbody>
</table>

© 2017 Cisco Systems, Inc. All Rights Reserved.
### Abbreviations

The following abbreviations 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>IT</td>
<td>Information Technology</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>

### Other Resources

In addition to this guide, you may find these documents and online resources useful.
Related Documents

Please refer to your Stealthwatch Documentation for information about Stealthwatch appliances and their installation and configuration. Please see Cisco Stealthwatch online for information about Stealthwatch products.

Additional information is available in the Stealthwatch Customer Community web site (http://community.lancope.com). If you do not have login access to the web site, send an email requesting access to Support.

Lancope Blog

Lancope’s Inside the Threat blog at http://www.lancope.com/blog/ provides a wealth of information about NetFlow, the NetFlow industry, and new Stealthwatch features, as well as tips and tricks on using Stealthwatch.

Lancope Resources & Tools for Advanced Cybersecurity

For further information about Stealthwatch, go to the Lancope Resources & Tools for Advanced Cybersecurity site https://www.lancope.com/resources. It includes resources such as an online video library, white papers, and Webinars.

Contacting Support

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

- Contact your local Cisco partner.
- Call +1 800-838-6574.
- Submit a case using the Support form on the Stealthwatch Customer Community web site (http://community.lancope.com)

Document Feedback

If you have comments about this document, please contact us at support@lancope.com. We appreciate your feedback.
INSTALLING A VIRTUAL APPLIANCE

Overview

Note: For instructions on how to install a Stealthwatch physical appliance, see the Stealthwatch System v6.x Hardware Installation Guide.

This chapter describes how to install the virtual appliances using VMware vSphere Client v4.x or later.

Note: Make sure the time set on the ESX server where you will be installing the virtual appliance reflects the correct time. Otherwise, the virtual appliances may not be able to boot up.

CAUTION! Do not install VMware Tools on a Stealthwatch virtual appliance because it will override the custom version already installed. Doing so would render the virtual appliance inoperable and require reinstallation.

Process Overview

Installing a virtual appliance involves completing the following procedures, which we discuss in this chapter:

1. Configuring Your Firewall for Communications
2. Logging in to the VMware vSphere Client
3. Adding a Resource Pool
4. Installing the Virtual Appliance

You must complete these procedures for the Flow Collector VE(s) first, and then do the same for the SMC VE(s).
Configuring Your Firewall for Communications

In order for the appliances to communicate properly, you should configure the network so that firewalls or access control lists do not block the required connections. Use the diagram and tables the table shown in this section to configure your network so that the appliances can communicate through the network.

Consult with your network administrator to ensure that the following ports are open and have unrestricted access:

- TCP 22
- TCP 25
- TCP 389
- TCP 443
- TCP 2393
- TCP 5222
- UDP 53
- UDP 123
- UDP 161
- UDP 162
- UDP 389
- UDP 514
- UDP 2055
- UDP 6343

Communication Ports

The following table shows how the ports are used in the Stealthwatch System:

<table>
<thead>
<tr>
<th>From (Client)</th>
<th>To (Server)</th>
<th>Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin User PC</td>
<td>All appliances</td>
<td>TCP/443</td>
<td>HTTPS</td>
</tr>
<tr>
<td>All appliances</td>
<td>Network time source</td>
<td>UDP/123</td>
<td>NTP</td>
</tr>
<tr>
<td>Active Directory</td>
<td>SMC</td>
<td>TCP/389, UDP/389</td>
<td>LDAP</td>
</tr>
<tr>
<td>AnyConnect</td>
<td>Endpoint Concentrator</td>
<td>UDP/2055</td>
<td>NetFlow</td>
</tr>
<tr>
<td>From (Client)</td>
<td>To (Server)</td>
<td>Port</td>
<td>Protocol</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------</td>
<td>--------</td>
<td>----------</td>
</tr>
<tr>
<td>Cisco ISE</td>
<td>SMC</td>
<td>TCP/443</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Cisco ISE</td>
<td>SMC</td>
<td>TCP/5222</td>
<td>XMPP</td>
</tr>
<tr>
<td>Endpoint Con-</td>
<td>Flow Collector</td>
<td>UDP/2055</td>
<td>NetFlow</td>
</tr>
<tr>
<td>- centra-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>tor</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>External log</td>
<td>SMC</td>
<td>UDP/514</td>
<td>SYSLOG</td>
</tr>
<tr>
<td>sources</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flow Collector</td>
<td>SMC</td>
<td>TCP/443</td>
<td>HTTPS</td>
</tr>
<tr>
<td>SLIC</td>
<td>SMC</td>
<td>TCP/443 or proxied connection</td>
<td>HTTPS</td>
</tr>
<tr>
<td>UDP Director</td>
<td>Flow Collector - sFlow</td>
<td>UDP/6343</td>
<td>sFlow</td>
</tr>
<tr>
<td>UDP Director</td>
<td>Flow Collector - NetFlow</td>
<td>UDP/2055*</td>
<td>NetFlow</td>
</tr>
<tr>
<td>UDP Director</td>
<td>3rd Party event management systems</td>
<td>UDP/514</td>
<td>SYSLOG</td>
</tr>
<tr>
<td>Flow Sensor</td>
<td>SMC</td>
<td>TCP/443</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Identity</td>
<td>SMC</td>
<td>TCP/2393</td>
<td>SSL</td>
</tr>
<tr>
<td>NetFlow Exporters</td>
<td>Flow Collector - NetFlow</td>
<td>UDP/2055*</td>
<td>NetFlow</td>
</tr>
<tr>
<td>sFlow Exporters</td>
<td>Flow Collector - sFlow</td>
<td>UDP/6343*</td>
<td>sFlow</td>
</tr>
<tr>
<td>SMC</td>
<td>Cisco ISE</td>
<td>TCP/443</td>
<td>HTTPS</td>
</tr>
<tr>
<td>SMC</td>
<td>DNS</td>
<td>UDP/53</td>
<td>DNS</td>
</tr>
<tr>
<td>SMC</td>
<td>Flow Collector</td>
<td>TCP/443</td>
<td>HTTPS</td>
</tr>
<tr>
<td>From (Client)</td>
<td>To (Server)</td>
<td>Port</td>
<td>Protocol</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>SMC</td>
<td>Flow Sensor</td>
<td>TCP/443</td>
<td>HTTPS</td>
</tr>
<tr>
<td>SMC</td>
<td>Identity</td>
<td>TCP/2393</td>
<td>SSL</td>
</tr>
<tr>
<td>SMC</td>
<td>Flow Exporters</td>
<td>UDP/161</td>
<td>SNMP</td>
</tr>
<tr>
<td>SMC</td>
<td>Endpoint Concentrator</td>
<td>UDP.2055</td>
<td>HTTPS</td>
</tr>
<tr>
<td>User PC</td>
<td>SMC</td>
<td>TCP/443</td>
<td>HTTPS</td>
</tr>
</tbody>
</table>

*This is the default NetFlow port, but any UDP port could be configured on the exporter.*

The following table is for optional configurations determined by your network needs:

<table>
<thead>
<tr>
<th>From (Client)</th>
<th>To (Server)</th>
<th>Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>All appliances</td>
<td>User PC</td>
<td>TCP/22</td>
<td>SSH</td>
</tr>
<tr>
<td>SMC</td>
<td>3rd Party event management systems</td>
<td>UDP/162</td>
<td>SNMP-trap</td>
</tr>
<tr>
<td>SMC</td>
<td>3rd Party event management systems</td>
<td>UDP/514</td>
<td>SYSLOG</td>
</tr>
<tr>
<td>SMC</td>
<td>Email gateway</td>
<td>TCP/25</td>
<td>SMTP</td>
</tr>
<tr>
<td>SMC</td>
<td>SLIC</td>
<td>TCP/443</td>
<td>SSL</td>
</tr>
<tr>
<td>User PC</td>
<td>All appliances</td>
<td>TCP/22</td>
<td>SSH</td>
</tr>
</tbody>
</table>

The following diagram shows the various connections used by the Stealthwatch System. The ports marked as *optional* may be used according to your own network needs.
Logging in to the VMware vSphere Client

To install the virtual appliance, you must first log in to the VMware vSphere Client, by completing the following steps:

**Note:** The screen images are for VMware v5.0 and may appear slightly different from your screens, but the commands are the same. If you use the VMware Web Client interface, some of the screens shown here will differ. Therefore, the differences in the options chosen will be pointed out where necessary.

1. Launch the VMware vSphere Client software. The Login dialog opens.
2. Type the IP address of the ESX server and your login credentials, and then click Login. The Home page opens.

Note: The Web Client has two dialogs for the configuration: Select name and location and Configure settings.

Adding a Resource Pool

A virtual appliance needs a resource pool with specific CPU and memory resources allocated to it so that it can operate without affecting other virtual machines. This procedure describes how to add a new resource pool with the proper allocations for a Stealthwatch virtual appliance.

Note: If desired, you can use an existing resource pool for a virtual appliance. However, you should examine this procedure to make sure the existing resource pool has enough resources allocated to it for a virtual appliance to operate properly. If you use the VMware Web Client v5.5 interface, some of the screens shown here will differ. Therefore, the differences in the options will be pointed out where necessary.

To add a resource pool for a virtual appliance on the ESX server where it will reside, complete the following steps:

1. In the Inventory tree on the left, right-click the ESX server IP address, and then select New Resource Pool from the popup menu or on the Web client select All vCenter Actions > New Resources Pool.
The Create Resource Pool dialog opens.

2. In the Name field, type the name you want to use to identify this resource group.
3. Do not change any of the settings in the CPU Resources section.
4. In the Memory Resources section, do the following:
   - Change the Reservation field as recommended in the chart for the applicable appliance in "Resource Requirements" on page 3.
   - Change the Limit field to at least 4 GB (8 GB recommended).
   - Click the Unlimited checkbox to clear it.

**CAUTION!** Less than 4 GB of memory is not supported. If less than 4 GB is allocated, a Low Memory alarm will be triggered, and no flows will be stored in the database.
7. Click OK. The resource pool appears beneath the ESX server on the Inventory tree.

8. Select the resource pool, and then click the Resource Allocation tab to review the CPU and memory resource allocations. On the Web Client, click the Manage tab and then click CPU Resources & Memory Resource.

9. Continue with the next section, Installing a Virtual Appliance

Installing the Virtual Appliance

To install a virtual appliance on the ESX server and define the virtual appliance management and monitoring ports, complete the following steps:

1. Unzip the virtual appliance software (OVF) file that you downloaded earlier.
2. On the vSphere client menu, click File > Deploy OVF Template. On the Web client, right-click the host, and then select Deploy OVF Template.
**Note:** The Web client OVF template wizard has slightly different wording and numbering for the steps of the procedure, but the steps are the same. One example is the Web client uses Source Location instead of Source. The image below shows the steps on the left side for a OVF template ready to deploy:

![Deploy OVF Template wizard](image)

The Deploy OVF Template wizard opens.

![Source page](image)

3. Click **Browse**, and then navigate to select the virtual appliance OVF file.
4. Click **Next** to display the OVF Template Details page (Web Client: 1.b. Review details).
5. Click **Next**. The End User License Agreement opens (1c. Accept EULAs).

6. After reviewing the information, click **Accept**, and then click **Next**. The Name and Location page opens (2a. Select name and folder).
7. If desired, change the name for the virtual appliance as it will appear in the Inventory tree, and then click **Next**.

   - If the Specify a Specific Host page opens, select the host or cluster where the virtual appliance will reside.

   - If the Host/Cluster page opens, select the host or cluster where the appliance will reside.
8. Click **Next**. The Resource Pool page opens.

9. Select the resource pool that you defined earlier, and then click **Next**.
   
   a. If the Datastore page opens, go to step 10.
   
   b. If the Disk Format page opens, go to step 11.

   **Note:** On the Web Client the Select storage page opens and includes both the datastore and the disk format.
10. On the Datastore page, select where you want to store the virtual appliance, and then click **Next**.

The Disk Format page opens.

**Note:** The vSphere Client v5 and later has two thick-provisioned formats: Lazy Zeroed and Eager Zeroed. Choose the one that best suits your disk storage needs. Use the Thin Provision format only if your disk space is limited. For further information, refer to your VMware documentation.

12. From the Destination Networks drop-down list, select a virtual appliance management port.

13. Click **Next**. The Ready to Complete page opens with a summary of the settings.
14. After reviewing the settings, click **Finish**. A progress dialog opens.

15. When the deployment is completed, click **Close** to close the progress dialog. The virtual appliance appears in the Inventory tree.

16. Have you completed all of the procedures in this chapter for all of the Flow Collector VEs and then all of the SMC VEs?

   - If yes, continue with **Configuring the Virtual Environment**
   - If no, repeat all of the procedures in this chapter for the next virtual appliance.
CONFIGURING THE VIRTUAL ENVIRONMENT

Overview

After you install the Stealthwatch VE appliances, you are ready to configure the virtual environment for them. This process involves completing the following procedures as detailed in this chapter:

1. Configure the IP Addresses
2. Change the Default User Passwords

You must complete these procedures for the Flow Collectors VEs first, and then do the same for the SMC VEs.

Configure the IP Addresses

To configure the IP addresses for a virtual appliance, complete the following steps:

1. If necessary, launch the vSphere Client software and log in. The Getting Started page opens.
2. In the Inventory tree, select the Stealthwatch virtual appliance you want to configure.
3. On the Getting Started page, click the “Power on the virtual machine” link. You may need to scroll down to see the link.

**Note:** If the virtual machine does not power on and you receive an error message about insufficient available memory, do one of the following:
- Increase the memory reservation limit for the appliance and its resource pool.
- Increase the available resources on the system where the appliance is installed.
- Decrease the memory allocation and reservation to 4 GB.

**CAUTION!** Do not reduce the memory reservation so that it is lower than the allocation, and never reduce the setting to less than 4 GB. For guidance, see the chart for the applicable appliance in “Resource Requirements” on page 3.

4. Click the **Console** tab. (On the Web client, click the Summary tab and then click the Launch Console link.) Allow the virtual appliance to finish booting up. The virtual appliance Administrative IP Address page opens.

5. Click on the page, and then enter the IP address for the virtual appliance.
6. Select **OK**, and then press **Enter**. The IP Netmask page opens with the default network mask IP address.
7. Do the following:
   - Accept the default value or enter a new one based on your environment.
   - Select OK and press Enter to continue.

   The IP Broadcast Address page opens with the default broadcast IP address.

8. Do the following:
   - Accept the default value or enter a new one based on your environment.
   - Select OK and press Enter to continue.

   The Gateway Address page opens with the default gateway server IP address.
9. Do the following:
   - Accept the default value or enter a new one based on your environment.
   - Select **OK** and press **Enter** to continue.

   A page opens showing a summary of your entries.

10. Review the information. Are the settings correct?
    - If yes, go to the next step.
    - If no, go to step 13.

11. Press **Enter**. The system restart page opens.
12. Press **Enter**. The system restarts and implements the changes. On completion, a login prompt appears.

13. Select **No** and press **Enter**. The Administrative IP Address page opens. Repeat steps 5 through 10 to make any necessary changes. The system restart page opens.

14. Press **Enter**. The system restarts and implements the changes. On completion, a login prompt appears.

15. Press **Ctrl + Alt** to exit the console.

16. Go to Change the Default User Passwords next in this chapter.

## Change the Default User Passwords

To ensure that your network is secure, you must change both the default passwords of the sysadmin and root passwords on the virtual appliance.

### Changing the sysadmin Password

To change the sysadmin password, complete the following steps:

1. At the login page, do the following:
a. When the password prompt appears, type `lan1cope`, and then press Enter.

b. Type `sysadmin` (case-sensitive), and then press Enter.

2. On the System Configuration menu, select Password and press Enter.

   ![System Configuration Menu]

   **Important:** If you change the trusted hosts list from the defaults, you must 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.

   ![Prompt for Current Password]

   A prompt for the current password appears below the menu.

3. Type the current password, and then press Enter.

   The prompt for a new password appears.
4. Type the new password, and then press Enter.

**Notes:**

- The password must be between 5 and 30 alphanumeric characters in length with no spaces. You also may use the following special characters: $.~!@#%_\=';\(\)
- Any password change must be different from the previous password by at least four characters.

5. Type the new password again, and then press Enter. A message appears indicating that the password was updated successfully.

6. Press Enter to return to the System Configuration Console menu.

7. Continue with the next section, “Changing the root Password.”
Changing the root Password

To change the root password, complete the following steps:

1. On the System Configuration Console menu, select **Advanced**, and then press **Enter**. The Advanced menu opens.

2. On the **Advanced** menu, select **RootShell**, and then press **Enter**.

   A prompt for the root password appears.

3. Type the current root password, **lan1cope**, and then press **Enter**. The root shell prompt appears.
4. Type **SystemConfig** (case-sensitive), and then press **Enter**.  
   This returns you to the System Configuration menu so that you can change the root password.

5. Select **Password**, and then press **Enter**. The password prompt appears.

6. Type the new root password, and then press **Enter**. A second prompt appears below the menu.

7. Retype the new root password, and then press **Enter**.
A message appears indicating that the password was updated successfully.

8. When your password change is successful, type exit, and then press Enter. You have now changed both of your default sysadmin and root passwords.

9. Press Ctrl+Alt to exit the console environment.

10. Have you completed all of the procedures in this chapter for all of the Flow Collector VEs and all the SMC VEs?

- If yes, continue with “Configuring a Virtual Appliance System.”
- If no, return to “Configure the IP Addresses” on page 25 and repeat all of the procedures in this chapter for the next virtual appliance. Then, go to the “Configuring a Virtual Appliance System.”
CONFIGURING A SYSTEM

Overview

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

Please refer to the checklist on “Before You Begin” on page 3 for the information you will need before proceeding.

Process Overview

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

1. Configuring the Individual Appliances
2. Configuring the System
3. Expand SMC VE or Flow Collector VE Disk Space
4. Increasing Memory for the Flow Collector VE
5. Configuration through the Appliance Admin Interface

Note: If you are using a failover SMC in your network, configure the failover appliance first. When you then configure the primary SMC, you will be able to set the failover SMC IP address.

You must complete these procedures for the Flow Collector VE(s) first, and then do the same for the SMC VE(s).

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. Depending on your system, you should configure the Flow Sensors and Flow Collectors before the UDP Directors, and then, lastly, configure the SMC VE. When you complete the initial setup for the SMC VE, the system setup tool opens and you can configure your Stealthwatch System.
Before you begin, gather the information detailed in the “Before You Begin” on page 3.

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

To configure, complete the following steps:

1. In the address field of your browser, type `https://` followed by the IP address of the virtual appliance, and then press **Enter**.
2. Are you configuring a SMC VE?
   - If yes, go to step 4.
   - If no, go to step 3.
3. The admin login page opens. Type **admin** and **lan411cope** (both are case sensitive), and then click **Login**. Go to step 5.

   ![Login Page](image)

To log in, do the following:

- In the User Name field, type **admin**.
- In the Password field, type **lan411cope**.
- Click **Sign In**.
5. The Welcome page opens. Click **Continue**.

![Welcome page](image1)

The Management Network Interface page opens.

![Management Network Interface](image2)

6. Review the settings you previously entered, and then click **Next**. The Password Management page opens.

![Password Management page](image3)
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"


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 VE last.
   - If no, go to the next step.
16. After configuring the last or only SMC VE, 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 VE 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 (VE) is added to the system:

![Flow Collector VE added](image)

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

![Appliance Flow Sensors page](image)

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](image)
9. Click the + button. The Add Flow Sensor dialogue appears:

![Add FlowSensor dialogue](image)

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

![Communication Established dialogue](image)

11. From the drop-down list select a Flow Collector, and then click Add. The Flow Sensor VE Login Credentials dialog opens.

![FlowSensor VE Login Credentials](image)

12. In the appropriate fields, type the following information needed for the Flow Sensor VE to communicate with the Flow Collector:
- VM Server Address
- Username of the Flow Sensor
- Password

13. Click **Add**.

The Flow Sensor is added.

14. Click **Next**. The SMTP Setting page opens:
15. Enter the email address that you want in the “from” field when the SMC sends emails.

16. Enter the SMTP Relay address, and then click Next. The SNMP Setting page opens:

17. If necessary, modify the settings (only one string can be set here), and then click Next.
18. The Internet Access (for the SMC) page opens.

19. Select the proper type of Internet access:

- **Direct access**: Your SMC is directly connected to the Internet (not through a proxy server). Click Next to open the Online page.

- **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.

  ![Internet Access Settings](image)

  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:

![Example Message]

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 59.

26. Are you configuring a SMC VE that collects external events (syslog) or a Flow Collector VE?
   - If yes, continue to the next section, “Expand SMC VE or Flow Collector VE Disk Space.”
   - If no, continue with “Configuration through the Appliance Admin Interface” on page 59.

---

### Expand SMC VE or Flow Collector VE Disk Space

This section includes the procedure for expanding the disk space of a SMC VE or a Flow Collector VE.

**Notes:**
- You do not need to expand the SMC VE disk space unless it is collecting external events (syslog).
- You cannot expand the SMC VE or Flow Collector VE disk space if you are using a Snapshot of the disk. You must remove the Snapshot first.

The SMC VE will use approximately 75% of the disk, leaving 25% free. Therefore, always expand the disk to 40% more than the desired disk amount.

The maximum data storage for the Flow Collector VE depends upon the model. The maximum amounts are as follows:
<table>
<thead>
<tr>
<th>Model</th>
<th>Maximum Disk Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flow Collector VE 1000</td>
<td>1 TB</td>
</tr>
<tr>
<td>Flow Collector VE 2000</td>
<td>2 TB</td>
</tr>
<tr>
<td>Flow Collector VE 4000</td>
<td>4 TB</td>
</tr>
</tbody>
</table>

To expand the virtual appliance disk space, complete the following steps:

1. In the Inventory tree, select the virtual appliance, and then click **Power Off the virtual machine**.

2. In the Inventory tree, right-click the virtual appliance in the Inventory tree, and then select **Edit Settings**.
3. From the Hardware list, select **Hard disk**. On the Web Client, expand the Hard disk 1 list. The disk information appears on the right.

4. In the Disk Provisioning section, enter the desired amount of disk space in the **Provisioned Size** field, and then click **OK**. The dialog closes.

5. Click the **Summary** tab to confirm that the storage amount has changed.
6. Click **Power On**.

7. Click the **Console** tab (on Web client, click the Launch Console link). Allow the virtual appliance to finish booting up. The Login page opens.

8. Click on the page, and then do the following:
   a. Type `sysadmin`, and then press **Enter**.
   b. When the password prompt appears, type `lan1cope`, and then press **Enter**.

The System Configuration menu opens.
9. Select the **Advanced** option, and then press **Enter**. The Advanced menu page opens.

10. Select the **DataStorageExpansion** option. The Data Storage Expansion page opens.
11. Review the information, then select **Yes**, and press **Enter**. The Warning page opens.

![Warning Page]

12. Select **Yes**, and then press **Enter**. The virtual appliance restarts and implements the changes.

13. Press **Ctrl+Alt** to exit the console environment.

14. Click the **Summary** tab and review the changes made to the data storage.

![Summary Tab]

15. Continue with the next section, “Increasing Memory for the Flow Collector VE.”
Increasing Memory for the Flow Collector VE

For the Flow Collector VE, you must increase the memory so its performance will be at the proper level.

The maximum memory for the Flow Collector VE depends upon the model. The maximum amounts are as follows:

<table>
<thead>
<tr>
<th>Model</th>
<th>Maximum Memory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flow Collector VE 1000</td>
<td>32 GB</td>
</tr>
<tr>
<td>Flow Collector VE 2000</td>
<td>64 GB</td>
</tr>
<tr>
<td>Flow Collector VE 4000</td>
<td>128 GB</td>
</tr>
</tbody>
</table>

To increase the memory level, complete the following steps:

1. Select the appliance.
2. Turn off the appliance, if necessary.
3. Right-click and select Edit Settings.
4. In the Hardware tab, select **Memory** (click to open Memory) and increase the memory size to 8 GB.

5. Click **OK** to apply the change. The interface returns to the Getting Started page.

6. Click **Power on the appliance** to restart the appliance. You will see a confirmation at the bottom of the page.

7. Continue with the section, "Configuration through the Appliance Admin Interface"
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. Restart the Virtual 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 9 and later and Firefox version 3 and later.
- If you have trouble loading any of the pages, 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 virtual appliance, and then press Enter.
2. Are you opening the SMC VE Appliance Admin interface?

   - If yes, the Landing page opens. In the upper right corner, click the Settings icon, and then click Administrator 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 virtual 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.

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 virtual appliance system time.

![Time Zone Configuration](image)

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.

![Time Zone Configuration](image)

4. Click Apply to make the changes permanent. The confirmation window opens.

![Confirmation Window](image)

5. Click OK.

6. Continue with the next section, Restart the Virtual Appliance.

**Restart the Virtual Appliance**

To restart the virtual appliance, complete the following steps:
1. On the Appliance Admin interface menu, select **Operations > Restart Appliance**.

   ![Restart Appliance](image)

   The confirmation dialog opens.

   ![Confirmation Dialog](image)

2. Click **Yes**.

9. Did you configure a SMC VE or a Flow Collector VE?

   - If it was a SMC VE, after restarting, it will begin communicating with the Flow Collectors. Congratulations, you have now completely installed and configured the virtual appliance! Please see the **SMC Client Online Help** for more information.
   - If it was a Flow Collector VE, continue to the next chapter, “**Verifying Communications**.”
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**

<table>
<thead>
<tr>
<th>Notes:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• You can add multiple independent Cisco ISE clusters to a domain.</td>
</tr>
<tr>
<td>• 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.</td>
</tr>
</tbody>
</table>

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.

© 2017 Cisco Systems, Inc. All Rights Reserved.
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.