Stealthwatch® Management Console VE and Flow Collector™ VE
Installation and Configuration Guide
(for Stealthwatch System v6.10.1)
Copyrights and Trademarks

© 2019 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

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contents</td>
<td>iii</td>
</tr>
<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>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>6</td>
</tr>
<tr>
<td>How to Use This Guide</td>
<td>8</td>
</tr>
<tr>
<td>Contacting Support</td>
<td>9</td>
</tr>
<tr>
<td>Installing a Virtual Appliance</td>
<td>11</td>
</tr>
<tr>
<td>Overview</td>
<td>11</td>
</tr>
<tr>
<td>Process Overview</td>
<td>11</td>
</tr>
<tr>
<td>Configuring Your Firewall for Communications</td>
<td>12</td>
</tr>
<tr>
<td>Communication Ports</td>
<td>12</td>
</tr>
<tr>
<td>Installing a Virtual Appliance using VMware vSphere Client</td>
<td>16</td>
</tr>
<tr>
<td>Overview</td>
<td>16</td>
</tr>
<tr>
<td>Before You Begin</td>
<td>16</td>
</tr>
<tr>
<td>Process Overview</td>
<td>16</td>
</tr>
<tr>
<td>Logging in to the VMware vSphere Client</td>
<td>17</td>
</tr>
<tr>
<td>Installing the Virtual Appliance</td>
<td>17</td>
</tr>
<tr>
<td>Installing a Virtual Appliance on a KVM Host</td>
<td>26</td>
</tr>
<tr>
<td>Overview</td>
<td>26</td>
</tr>
<tr>
<td>Before You Begin</td>
<td>26</td>
</tr>
<tr>
<td>Process Overview</td>
<td>26</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Installing a Virtual Appliance on a KVM Host</td>
<td>27</td>
</tr>
<tr>
<td><strong>Configuring the Virtual Environment</strong></td>
<td>33</td>
</tr>
<tr>
<td>Overview</td>
<td>33</td>
</tr>
<tr>
<td>Configure the IP Addresses</td>
<td>33</td>
</tr>
<tr>
<td>Change the Default User Password</td>
<td>37</td>
</tr>
<tr>
<td>Changing the sysadmin Password</td>
<td>37</td>
</tr>
<tr>
<td>Changing the root Password</td>
<td>39</td>
</tr>
<tr>
<td><strong>Configuring a System</strong></td>
<td>43</td>
</tr>
<tr>
<td>Overview</td>
<td>43</td>
</tr>
<tr>
<td>Process Overview</td>
<td>43</td>
</tr>
<tr>
<td>Configuring the Individual Appliances</td>
<td>43</td>
</tr>
<tr>
<td>Configuring the System</td>
<td>50</td>
</tr>
<tr>
<td>Expand Data Storage and Resource Allocations</td>
<td>60</td>
</tr>
<tr>
<td>Configuration through the Appliance Admin Interface</td>
<td>62</td>
</tr>
<tr>
<td>Log in to the Appliance Administration Interface</td>
<td>63</td>
</tr>
<tr>
<td>Configure the System Time</td>
<td>65</td>
</tr>
<tr>
<td>Restart the Virtual Appliance</td>
<td>66</td>
</tr>
<tr>
<td><strong>Verifying Communications</strong></td>
<td>69</td>
</tr>
<tr>
<td>Overview</td>
<td>69</td>
</tr>
<tr>
<td>Verify NetFlow Data Collection</td>
<td>69</td>
</tr>
<tr>
<td><strong>Adding Cisco ISE</strong></td>
<td>71</td>
</tr>
<tr>
<td>Overview</td>
<td>71</td>
</tr>
<tr>
<td>Add a Cisco ISE</td>
<td>71</td>
</tr>
<tr>
<td><strong>Enabling the SLIC Threat Feed</strong></td>
<td>73</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.

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 or KVM.

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 virtual 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.

© 2019 Cisco Systems, Inc. All Rights Reserved.
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 VMware vSphere client interface or KVM interface, and then the Appliance Administration (Admin) interface.

Compatibility

You can use VMware or KVM (Kernel-based Virtual Machine) for the virtual appliance installation. It is important to review the following compatibility information:

VMware

- **Compatibility**: VMware vSphere v5.5 or 6.0
- **VMware Upgrades**: Stealthwatch VE appliances that are running on older versions of VMware ESX are not compatible with ESX v5.5 or 6.0. If you upgrade VMware to ESX v5.5 or 6.6, delete your existing Stealthwatch VE appliances and reinstall them.
- **Live migration** (for example, with vMotion) from host to host is not supported.
- **Virtual machine snapshots** are not supported.

**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.

KVM Using Any Compatible Linux Distribution

- **KVM Host Versions**: There are several methods used to install a virtual machine on a KVM host. We tested KVM and validated performance using the following components:
  
  ```
  libvirt 3.0.0
  qemu-KVM 2.8.0
  Open vSwitch 2.6.1
  Linux Kernel 4.4.38
  ```

- **Virtualization Host**: For minimum requirements and best performance, review the Resource Requirements section and see the hardware specification sheet for your appliance at [Cisco.com](http://Cisco.com).

  **Note**: The system performance is determined by the host environment. Your performance may vary.

Installation Order

It is important to install and configure your virtual appliances in the following order:
1. UDP Director
2. Flow Collector Database 5000 Console (if used)
3. All other Flow Collectors
4. All Flow Sensors
5. Cloud License Concentrator
6. Endpoint Concentrator
7. Secondary Stealthwatch Management Console
8. Primary Stealthwatch Management Console

If you do not follow this recommended order when you set up the Stealthwatch system, the 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 virtual host server (where you will be installing the virtual appliances) reflects 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 appliance installation file (OVF or ISO) from the Download and License Center. For instructions on downloading the file for each appliance, see the *Downloading and Licensing Stealthwatch Products* document in the Download and License Center or on Cisco.com.

**Registering and Licensing**

As part of the configuration process, you will register and license your Stealthwatch products. For instructions, see the *Downloading and Licensing Stealthwatch Products* document in the Download and License Center or on Cisco.com.

**Resource Requirements**

This section provides the resource requirements for the virtual appliances. You can use the tables provided in this section to record settings you will need to install and configure the Stealthwatch VE appliances.

**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 or ISO</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>
</tbody>
</table>

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

These are the Stealthwatch Management Console VE models and their capacities:

<table>
<thead>
<tr>
<th>SMC VE Model</th>
<th>Reserved Memory</th>
<th>Reserved CPUs</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMC VE</td>
<td>≤ 63 GB</td>
<td>up to 7</td>
</tr>
<tr>
<td>SMC VE 2000</td>
<td>≥ 64 GB</td>
<td>8 or more</td>
</tr>
</tbody>
</table>

**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:
### Flows 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>Flow Collector VE Model</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>FCVE</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>≥ 33 GB and ≤ 65 GB</td>
<td>6</td>
<td>2000</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>≥ 66 GB</td>
<td>7</td>
<td>4000</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 Samsung 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

During installation, you will expand the available data storage on the server. Use the following information to allocate the correct amount of storage for each appliance.

- **Expansion Calculation:** The virtual appliance uses approximately 75% of the server for data storage, leaving 25% for the operating system and cache. Therefore, always expand...
the data storage to 40% more than the desired amount.

- **FPS Calculation:** Cisco recommends allocating a minimum of 1 GB of data storage for 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 data storage space.

- **If the External Event processing (syslog) feature is used,** more memory and processing resources are required.

- **Minimum Data Storage:** Use the following table to determine the minimum data storage required for each appliance. To install the appliance, you will expand the data storage space (see Expand Data Storage and Resource Allocations for details).

<table>
<thead>
<tr>
<th>Stealthwatch VE Model</th>
<th>Minimum Data Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stealthwatch Management Console VE</td>
<td>100 GB</td>
</tr>
<tr>
<td>Stealthwatch Management Console VE 2000</td>
<td>200 GB</td>
</tr>
<tr>
<td>Flow Collector NetFlow VE</td>
<td>200 GB</td>
</tr>
<tr>
<td>Flow Collector NetFlow VE 2000</td>
<td>600 GB</td>
</tr>
<tr>
<td>Flow Collector NetFlow VE 4000</td>
<td>1.5 TB</td>
</tr>
<tr>
<td>Flow Collector sFlow VE</td>
<td>100 GB</td>
</tr>
<tr>
<td>Flow Collector sFlow VE 2000</td>
<td>600 GB</td>
</tr>
<tr>
<td>Flow Collector sFlow VE 4000</td>
<td>1.5 TB</td>
</tr>
<tr>
<td>Flow Sensor</td>
<td>50 GB</td>
</tr>
<tr>
<td>UDP Director</td>
<td>50 GB</td>
</tr>
</tbody>
</table>

### Information Needed for Console Access

<table>
<thead>
<tr>
<th>Setting</th>
<th>Hypervisor 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>(Default = 192.168.1.11)</td>
<td></td>
</tr>
<tr>
<td>Netmask IP Address</td>
<td>(Default = 255.255.255.0)</td>
<td>(Default = 255.255.255.0)</td>
<td></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>Gateway IP Address</td>
<td>(Default = 192.168.1.1)</td>
<td>(Default = 192.168.1.1)</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. Installing a Virtual Appliance</td>
<td>How to prepare the virtual environment and install VE appliances</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>
<tr>
<td>5. Verifying Communications</td>
<td>How to verify that the SMC is receiving NetFlow data</td>
</tr>
<tr>
<td>6. Adding Cisco ISE</td>
<td>How to add an identity device</td>
</tr>
<tr>
<td>7. Enabling the SLIC Threat Feed Feature</td>
<td>How to enable the SLIC Threat Feed feature in the SMC client interface</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>
</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.)
INSTALLING A VIRTUAL APPLIANCE

Overview

This chapter describes how to install the virtual appliances.

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

Compatibility: You can use one of the following for the virtual edition installation. For compatibility details, see the Compatibility section of the Introduction.

- VMware vSphere Client v5.5 or 6.0
- KVM using any Linux distribution

**Note:** Confirm the time setting on the virtual host server (where you will be installing the virtual appliances) reflects the correct time. Otherwise, the 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. Installing a Virtual Appliance using VMware vSphere Client or KVM.

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 information provided 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>centrator</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 Con-</td>
<td>UDP.2055</td>
<td>HTTPS</td>
</tr>
<tr>
<td></td>
<td>centrator</td>
<td></td>
<td></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</td>
<td>UDP/162</td>
<td>SNMP-trap</td>
</tr>
<tr>
<td></td>
<td>management systems</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMC</td>
<td>3rd Party event</td>
<td>UDP/514</td>
<td>SYSLOG</td>
</tr>
<tr>
<td></td>
<td>management systems</td>
<td></td>
<td></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.
Note: Go to the section that is applicable to your virtual appliance installation: VMware vSphere Client or KVM.
Installing a Virtual Appliance using VMware vSphere Client

Overview

This chapter describes how to install the virtual appliances using VMware vSphere Client (v5.5 or 6.0).

Before You Begin

Before you begin the installation, complete the following preparation procedures:

1. Download the OVF file from the Download and License Center. See the Downloading and Licensing Guide for instructions.
2. Review the Compatibility information in the Introduction.
3. Configure Your Firewall for Communications.
4. Review the Resource Requirements section to determine the proper allocations for the appliance. You can use a resource pool or alternative method to allocate resources.
5. Confirm 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.

WARNING! Do not install an untrusted physical or virtual machine on the same physical cluster/system as your Stealthwatch System appliances.

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 are covered in this chapter:

1. Logging in to the VMware vSphere Client
2. Installing the Virtual Appliance
Logging in to the VMware vSphere Client

To install the virtual appliance, you must first log in to the VMware vSphere Client (v5.5 or 6.0), by completing the following steps:

**Note:** Whether you are using the The VMware vSphere Client or Web Client interface, some of the graphics and commands may vary from the information shown here. Please see your VMware vSphere guide for details related to the software.

1. Launch the VMware vSphere Client software. The Login dialog opens.

   ![Login dialog](image)

2. Type the IP address of the ESX server and your login credentials.
3. Click **Login**. The Home page opens.

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

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. Locate the virtual appliance software file (OVF.TGZ) that you downloaded from the Download and License Center.
2. Unzip or open the file, and then untar it.
   - To untar the file, select all the files in the folder and extract them.
   - Unzipping TGZ file is a two-step process, and the steps may vary depending on the software you use.
3. On the vSphere client menu, click **File > Deploy OVF Template**.
   - **Web Client:** Right-click the host. Select **Deploy OVF Template**.

© 2019 Cisco Systems, Inc. All Rights Reserved.
The Web client OVF template wizard may vary from the images and instructions shown here, but the steps are similar. 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:

The Deploy OVF Template wizard opens.
4. Click **Browse**. Navigate to select the virtual appliance OVF file.
5. Click **Next** to display the OVF Template Details page.

**Web Client:** The 1.b. Review details page opens.
6. Click **Next**. Review the End User License Agreement.
   **Web Client**: 1c. Accept EULAs.

7. After reviewing the information, click **Accept**. Click **Next**. The Name and Location page opens.
   **Web Client**: 2a. The Name and Location page opens.
8. **Optional**: Change the name and location for the virtual appliance. This should be a unique name and will display in the Inventory tree. Click **Next**.

9. On the Storage page, select where you want to store the data files. Click **Next**.
10. On the Disk Format page, select **Thick Provision Lazy Zeroed** or **Thick Provision Eager Zeroed**. Click **Next**.
   - Use the Thin Provision format only if your disk space is limited.
   - For more information, see your VMware documentation.
11. On the Network Mapping page, select the networks for the virtual appliance. Click **Next**.

**Web Client:** The 2c. Setup Networks page opens.
12. On the Ready to Complete page, review the summary of settings. If they are correct, click Finish.
13. The deployment dialog box opens.

14. When the deployment is completed, click **Close**. The installed virtual appliance appears in the Inventory tree.
15. 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, go to Configuring the Virtual Environment
   - If no, repeat all of the procedures in this chapter for the next virtual appliance.

# INSTALLING A VIRTUAL APPLIANCE ON A KVM HOST

## Overview

This chapter describes how to install the virtual appliances using **KVM and Virtual Machine Manager**.

## Before You Begin

Before you begin the installation, complete the following preparation procedures:

1. Download the ISO file from the Download and License Center and copy the image to a folder on the KVM host. In the example given below, the folder is var/lib/libvirt/image. See the *Downloading and Licensing Guide* for instructions.
2. Review the Compatibility information in the **Introduction**.
3. **Configure Your Firewall for Communications**.
4. Review the **Resource Requirements** section to determine the proper allocations for the appliance.
5. Confirm the time set on the virtual host server (where you will be installing the virtual appliance) reflects the correct time. Otherwise, the virtual appliances may not be able to boot up.

**WARNING!** Do not install an untrusted physical or virtual machine on the same physical cluster/system as your Stealthwatch System appliances.

## Process Overview

Installing a virtual appliance involves completing the following procedures, which are covered in this chapter:
Installing a Virtual Appliance on a KVM Host

There are several methods to install a virtual machine on a KVM host using a ISO file. The following steps give one example for installing a virtual SMC appliance through a GUI tool called Virtual Machine Manager running on a Ubuntu box. You can use any compatible Linux distribution. For compatibility details, see the Compatibility section of the Introduction.

To install a virtual appliance, complete the following steps:

1. Use Virtual Machine Manager to connect to the KVM Host.
2. Click **File > New Virtual Machine**.
3. Select **Local install media (ISO image or CDROM)**, and then click **Forward**.
4. Click **Use ISO image**.
5. Click **Browse**. Select the appliance image.
6. Select the ISO file. Click **Choose Volume**.

   **Note:** Confirm the ISO file is accessible by the KVM Host.

7. Under **Choose an operating system type and version**, select **Linux** from the OS type drop-down list.

8. From the Version drop-down list, select **Debian Jessie**. Click **Forward**.
9. Increase the Memory (RAM) and CPUs to the amount shown in the Resource Requirements section.

10. Click Forward.

11. Select Create a disk image for the virtual machine.

12. Enter the data storage amount shown for the appliance in the Resource Requirements section. Click Forward.
13. Assign a Name for the virtual machine. This will be the display name, so use a name that will help you find it later.

14. Select the **Customize configuration before install** check box.

15. In the Network selection drop-down box, select the applicable network and port group for installation.

16. Click **Finish**. The configuration menu opens.
17. In the navigation pane, select **NIC**.
18. Under Virtual Network Interface, select **e1000** in the Device model drop-down box. Click **Apply**.
19. Click VirtIO Disk 1.
20. In the Advanced Options drop-down list, select SCSI in the Disk bus drop-down box.
   Click Apply.
21. Click Begin Installation.
22. Go to Configuring the Virtual Environment.
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. Connect to your Hypervisor host (virtual machine host).
2. In the Hypervisor host, locate your virtual machine.
3. Confirm the virtual machine is powered on.

**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 available resources on the system where the appliance is installed. See the [Resource Requirements](#) section for details.
- **ESX server**: Increase the memory reservation limit for the appliance and its resource pool.

4. Access the virtual machine console.
5. Allow the virtual appliance to finish booting up. The virtual appliance Administrative IP Address page opens.
6. Click on the page. Enter the IP address for the virtual appliance.
7. Select OK, and then press Enter. The IP Netmask page opens with the default network mask 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 IP Broadcast Address page opens with the default broadcast 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.

   The Gateway Address page opens with the default gateway server IP address.

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

12. Press Enter. The system restart page opens.

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

14. 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.

15. Press Enter. The system restarts and implements the changes. On completion, a login prompt appears.
16. Press Ctrl + Alt to exit the console.
17. Go to Change the Default User Passwords next in this chapter.

Change the Default User Passwords

**Important:** To ensure that your network is secure, you must change the default password for the sysadmin and root users.

Changing the sysadmin Password

To change the sysadmin password, complete the following steps:

1. At the login page, do the following:
   a. Type sysadmin (case-sensitive), and then press Enter.
   b. When the password prompt appears, type lan1cope, and then press Enter.

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

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 8 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.

![Advanced menu screenshot](image)

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 and repeat all of the procedures in this chapter for the next virtual appliance. Then, go to the Configuring a 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.

Note: 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 Data Storage and Resource Allocations
4. 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.

It is important to install and configure your virtual appliances in the following order:
1. UDP Director VE
2. Flow Collector Database 5000 Console (if used)
3. All other Flow Collectors
4. All Flow Sensors
5. Cloud License Concentrator
6. Endpoint Concentrator
7. Secondary Stealthwatch Management Console
8. Primary Stealthwatch Management Console

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:
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. Review the settings you previously entered, 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.

![Notice](image)

**Notice**

This appliance will now restart. Are you sure you want to continue?

[OK]

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, 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:

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

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

![Add Flow Sensors Dialogue]

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

![Communication Established Dialogue]

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

![Flow Sensor VE Login Credentials Dialogue]

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 page opens:

17. 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.

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.

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)

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 62.

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 Data Storage and Resource Allocations.”
   - If no, continue with “Configuration through the Appliance Admin Interface” on page 62.

## Expand Data Storage and Resource Allocations

To install a virtual appliance, you may need to expand the available data storage. Also, you may want to expand the appliance resource allocations to improve performance. This procedure is required for the Flow Collector VE.

- For data storage ranges and resource allocation information, see the Resource Requirements: Data Storage section.
- For the **Flow Collector VE**, you must increase the memory so its performance will be at the proper level.
- If you increase the virtual machine memory using another method on your Hypervisor host, restart the appliance after you have saved your changes.

To expand the virtual appliance data storage, complete the following steps:
Note: You cannot expand the SMC VE or Flow Collector VE data storage if the virtual machine has any associated snapshots. Before you start the data storage expansion, remove the snapshots.

1. Connect to your Hypervisor host (virtual machine host).
2. In the Hypervisor host, locate your virtual machine.
3. Power off the virtual machine.
4. Access the virtual machine console.
5. 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.

6. Select the Advanced option, and then press Enter. The Advanced menu page opens.
7. Select the **DataStorageExpansion** option. The Data Storage Expansion page opens.

8. Review the information and change it as needed. To save your changes, select **Yes**, and press **Enter**. The Warning page opens.

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

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

11. Confirm the changes made to the data storage.

### 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 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 virtual 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 VE 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 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.

© 2019 Cisco Systems, Inc. All Rights Reserved.
2. Scroll down to the Time Zone section of the page to configure the virtual 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.

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:

The confirmation dialog opens.

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

### 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

To enable the SLIC Threat Feed through the SMC Desktop Client, complete the following steps:

1. Configure your firewall to allow the following:

   **IP Ranges:**
   - 64.14.29.0/24
   - 64.27.162.0/24

   **Fully Qualified Domain Name:**
   - lancope.flexnetoperations.com

2. Open the primary SMC Desktop Client.

3. In the SMC Enterprise tree, right-click the Stealthwatch Labs Intelligence Center branch. Select **Configuration > SLIC Threat Feed Configuration.**

   ![SLIC Threat Feed Configuration dialog](image)

   The SLIC Threat Feed Configuration dialog opens.
4. Check the **Enable the SLIC Threat Feed** check box.

5. In the **SLIC Feed Key** field, type your key.

6. 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 so far.

**Help:** Refer to Stealthwatch Desktop Client Online Help for more information about SLIC Threat Feed.

For further assistance, refer to the Stealthwatch Management Console User's Guide or the Desktop Client interface online Help.

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