Stealthwatch®

Flow Sensor™ Virtual Edition
Installation and Configuration Guide
(for Stealthwatch System v6.9.0)
Installation and Configuration Guide: Flow Sensor VE v6.9.0
© 2017 Cisco Systems, Inc. All rights reserved.

Document Date: February 2, 2017

Cisco Trademark

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)
CONTENTS

Contents .............................................................................................................................. iii

Introduction ........................................................................................................................ 1
  Overview ......................................................................................................................... 1
  Audience .......................................................................................................................... 1
  About the Flow Sensor VE ............................................................................................. 1
  Before You Begin ............................................................................................................. 2
  How to Use This Guide .................................................................................................. 5
  Other Resources ............................................................................................................. 6

Installing a Virtual Appliance ............................................................................................ 9
  Overview ......................................................................................................................... 9
  Process Overview ........................................................................................................... 9
  Configuring Your Firewall for Communications ............................................................ 10
    Communication Ports .................................................................................................. 10
  Logging in to the VMware vSphere Client ...................................................................... 13
  Adding a Distributed Virtual Port Group ....................................................................... 14
  Adding a Resource Pool ................................................................................................ 18
  Adding a Promiscuous Port Group ............................................................................... 21
    Add a Port Group ......................................................................................................... 21
    Set the Port Group to Promiscuous Mode .................................................................. 25
  Installing the Virtual Appliance .................................................................................... 28
  Defining Additional Monitoring Ports .......................................................................... 36

Configuring the Virtual Environment ................................................................................ 41
  Overview ......................................................................................................................... 41
  Configure the IP Addresses ............................................................................................ 41
  Change the Default User Passwords .............................................................................. 45
Changing the sysadmin Password ......................................................................................... 45
Changing the root Password ............................................................................................... 47

Configuring a Virtual Appliance .......................................................................................... 51

Overview ............................................................................................................................... 51
Process Overview ................................................................................................................ 51
Configuring the Individual Appliances ................................................................................ 51
Increasing Memory for the Flow Sensor VE ........................................................................ 56
Configuration through the Appliance Admin Interface ....................................................... 58
Log in to the Appliance Administration Interface ............................................................. 59
Configure the System Time .................................................................................................. 59
Restart the Virtual Appliance ............................................................................................... 61
INTRODUCTION

Overview

This is an installation and configuration guide for the Flow Sensor 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 Sensor 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 Flow Sensor VE appliances. This guide assumes the audience has a basic familiarity with VMware software.

**About the Flow Sensor VE**

Using the same technology as the Stealthwatch Flow Sensor appliance, the Flow Sensor VE is a virtual appliance that provides visibility into VMware environments, generating flow data for areas that are not flow-enabled.
As a virtual appliance installed inside each vSphere/ESX host, the Flow Sensor VE connects promiscuously to the virtual switches. Once installed, the Flow Sensor VE passively captures Ethernet frames from the traffic it observes and creates flow records containing valuable session statistics that pertain to conversational pairs, bit rates, and packet rates. The Flow Sensor VE then sends these records to any flow collector that supports NetFlow v9.

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

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

**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

This section provides the resource requirements for the virtual appliances.

**Flow Sensor VE**

The Stealthwatch System beginning with v6.8.0 offers various types of Flow Sensor VEs depending upon the number of NICs for the Flow Sensor VE. All VE appliance deployments should start at 50 GB of disk space.

<table>
<thead>
<tr>
<th>NICs - monitoring ports</th>
<th>Reserved CPUs</th>
<th>Reserved Memory</th>
<th>Throughput</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flow Sensor VE</td>
<td>1</td>
<td>1</td>
<td>4 GB</td>
</tr>
</tbody>
</table>

**Flow Sensor VE**

The Stealthwatch FlowSensor VE requires that the VMware server meets the following specifications:
- 4096 MB RAM
- 4 GB disk space (8 GB is recommended.)

**Note:** A vNetwork Distributed Switch (VDS) environment requires one resource pool with 512 MB RAM for each Flow Sensor VE.

**Flow Sensor VE Network Environments**

Before installing the Flow Sensor VE, you must know the type of network environment you have. This guide covers all types of network environments that a Flow Sensor VE can monitor. The main distinction is whether a network uses a VDS.

**Note:** Stealthwatch supports a VDS environment, but it does not support VMware Distributed Resource Scheduler (VM-DRS).

The Flow Sensor VE monitors the following types of VDS network environments:

- A network with virtual local area network (VLAN) trunking
- Discrete VLANs where one or more VLANs are prohibited from attaching packet monitoring devices (for example, due to local policy)
- Private VLANs
- ESX hosts rather than VLANs

**Information Needed for the vSphere Client Interface**

<table>
<thead>
<tr>
<th>Setting</th>
<th>ESX/vSphere Server</th>
<th>Flow Sensor VE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login User Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Login Password</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td></td>
<td>(Default = 192.168.1.6)</td>
</tr>
<tr>
<td>Netmask IP Address</td>
<td></td>
<td>(Default = 255.255.255.0)</td>
</tr>
<tr>
<td>Gateway IP Address</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 Sensor VE</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>(Default = 192.168.1.6)</td>
</tr>
</tbody>
</table>
The Flow Sensor VE requires the following additional information:

IP addresses and listening port numbers (default = 2055) for each NetFlow collector and/or UDP Director™ that will be receiving data from the Flow Sensor VE.

### 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>Installing a Virtual Appliance</td>
<td>How to install VE appliances on an ESX server using vSphere Client v4.x or later</td>
</tr>
<tr>
<td>Configuring the Virtual Environment</td>
<td>How to set up the virtual environment for the appliances</td>
</tr>
<tr>
<td>Configuring a Virtual Appliance System</td>
<td>How to configure appliances to begin processing traffic data</td>
</tr>
</tbody>
</table>

### 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>Abbreviations</td>
<td>Definition</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------</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](http://www.lancope.com/blog/) online for information about Stealthwatch products.

Additional information is available in the Lancope Community web site ([https://lancope.force.com/Customer/CustomerCommLogin](https://lancope.force.com/Customer/CustomerCommLogin)). If you do not have login access to the web site, send an email requesting access to [Support](http://www.lancope.com/blog/).

**Lancope Blog**

Lancope's *Inside the Threat* blog at [http://www.lancope.com/blog/](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](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.

**Document Feedback**

If you have comments about this document, please contact us at [support@lancope.com](mailto: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 Distributed Virtual Port Group
4. Adding a Resource Pool
5. Adding a Promiscuous Port Group
6. Installing the Virtual Appliance
7. Defining Additional Monitoring Ports
**Important:** If your network has a vNetwork Distributed Switch (VDS), then you must do Step 3 to add a dvPort group. If your network does not have a VDS, then do step 5 to add a promiscuous port group.

## 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>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>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>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 Concentrator</td>
<td>Flow Collector</td>
<td>UDP/2055</td>
<td>NetFlow</td>
</tr>
<tr>
<td>External log sources</td>
<td>SMC</td>
<td>UDP/514</td>
<td>SYSLOG</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 -</td>
<td>UDP/6343*</td>
<td>sFlow</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>sFlow</td>
<td></td>
<td></td>
<td></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>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.

3. Continue with the next section, **Adding a Resource Pool**

4. Are you installing a Flow Sensor VE in a VDS environment? (For further information about a VDS environment, see .

   - If yes, continue with the next section, **Adding a Distributed Virtual Port Group**
   - If no, continue with “**Adding a Resource Pool**” on page 18.

## Adding a Distributed Virtual Port Group

**Note:** This section applies only to VDS networks. If your network is in a non-VDS environment, go to **Adding a Resource Pool**

In a network using a VDS, you need to add a distributed virtual port (dvPort) group with the correct VLAN settings for each VDS that the Flow Sensor VE will monitor.

**Note:** If your environment uses a VLAN (other than VLAN trunking or a private VLAN), you will need the VLAN identifier to complete this procedure. If the Flow Sensor VE monitors both VLAN and non-VLAN traffic on the network, you need to create two dvPort groups, one for each type.

To add a dvPort group, complete the following steps:

1. In the **View** menu, select **Inventory > Networking** to display the Networking tree on the left.
On the Web client, click **Networking** in the Inventory Trees list:

2. In the Networking tree, select the VDS.

3. In the right pane, click **Create a new port group**.

The Create dvPort Group wizard opens.
Note: The Web Client has two dialogs for the configuration: Select name and location and Configure settings.

4. In the Name field, type the name you want to use to identify this dvPort group.
5. In the Number of Ports field, type the number of Flow Sensor VEs in your cluster of hosts.
6. Does your environment use a VLAN?
   - If yes, select the VLAN type from the drop-down list. Then, go to Step 7.
   - If no, select None from the VLAN type drop-down list. Then, go to step 8.
7. Based on the VLAN type you selected, perform the action indicated in the following table:

<table>
<thead>
<tr>
<th>VLAN Type</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>In the VLAN ID field, enter the number (between 1 and 4094) that matches the identifier.</td>
</tr>
<tr>
<td>VLAN Trunking</td>
<td>In the VLAN trunk range field, enter 0-4094 to monitor all VLAN traffic.</td>
</tr>
<tr>
<td>Private VLAN</td>
<td>Select Promiscuous from the drop-down list.</td>
</tr>
</tbody>
</table>
8. Click **Next**. A Summary page opens.

![Create Distributed Virtual Port Group dialog](image)

9. After reviewing the settings, click **Finish**. The new dvPort group appears in the Networking tree.

![Networking tree with dvPort group](image)

10. Right-click the new dvPort group and select **Edit Settings**.

![Right-click options](image)

The Settings dialog opens.
11. In the left pane, select **Security**.
12. In the right pane in the Promiscuous Mode drop-down list, select **Accept**.
13. Click **OK** to close the dialog.
14. Does the Flow Sensor VE monitor both VLAN and non-VLAN network traffic?
   - If yes, repeat steps through to add a dvPort group.
   - If no, continue to the next step.
15. Is there another VDS on the ESX server that the Flow Sensor VE will monitor?
   - If yes, repeat steps through for the next VDS.
   - If no, continue with the next section.

## 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 appliance in “Resource Requirements” on page 3.
• 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. Are you installing a Flow Sensor VE in a non-VDS environment? (For further information about network environments, see .)
   • If yes, continue with the next section, “Adding a Promiscuous Port Group .”
   • If no, continue to “Installing the Virtual Appliance” on page 28.
Adding a Promiscuous Port Group

**Note:** This section applies only to non-VDS networks. If your network uses a VDS, go to “Installing a Virtual Appliance” on page 9.

After defining a resource pool with the proper resource allocations, you must add a promiscuous port group for each virtual switch that the Flow Sensor VE will be monitoring. This addition involves completing these two procedures:

1. Add a Port Group
2. Set the Port Group to Promiscuous Mode

Add a Port Group

To add a port group, complete the following steps:

1. In the Inventory tree, select the ESX server, and then click the **Configuration** tab.

The Configuration page opens.
2. In the Hardware pane, click **Networking**.

The Configuration tab displays the list of installed virtual switches.

3. Scroll through the list to locate the virtual switch that the Flow Sensor VE will be monitoring, and then click the **Properties** link. The Properties dialog for that virtual switch opens.
4. Click **Add**. The Add Network Wizard opens to the Connection Type page.

5. Under **Connection Types**, select **Virtual Machine**, and then click **Next**. The Connection Settings page opens.
6. If desired, change the **Network Label** for the port group.

7. Click the **VLAN ID** drop-down list and select **All (4095)** to allow the Flow Sensor VE to see traffic on all VLANs through this port group.

8. Click **Next**. The Summary page opens, showing the port group you added.
9. Click **Finish** to return to the virtual switch Properties dialog, which shows the new port group.

![Virtual Switch Properties](image)

10. Continue with the next section.

**Set the Port Group to Promiscuous Mode**

To set the port group to Promiscuous Mode, complete the following steps:

1. On the virtual switch Properties dialog, select the port group you just added and click **Edit**.
The Properties dialog for the port group opens.

2. Click the **Security** tab to display the **Policy Exceptions** options.
3. Click the **Promiscuous Mode** checkbox, and then select **Accept** from the drop-down list.
4. Click **OK** to return to the virtual switch Properties dialog.
5. Click **Close** to dismiss the virtual switch Properties dialog. The new port group appears on the Networking page of the Configuration tab.
6. Will the Flow Sensor VE be monitoring another virtual switch on this ESX server?

   - If yes, go back to “Add a Port Group” on page 21, and repeat all the steps for the next virtual switch.
   - If no, continue with the next section, "Installing the 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:

The Deploy OVF Template wizard opens.

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. Are you installing a Flow Sensor VE, which will be monitoring more than one virtual switch on an ESX server or more than one VDS in a cluster?
   - If yes, continue with the next section, “Defining Additional Monitoring Ports.”
• If no, continue with Configuring a Virtual Appliance System on page 51.

**Defining Additional Monitoring Ports**

**Note:** This procedure is necessary *only* if the Flow Sensor VE will be monitoring more than one virtual switch on an ESX server or more than one VDS in a cluster.

To add Flow Sensor VE monitoring ports, complete the following steps:

1. In the Inventory tree, right-click the Flow Sensor VE, and then select **Edit Settings**.

![Image](image.png)

2. Click Add. The Add Hardware dialog opens to the Device Type page.

3. Select Ethernet Adapter in the list of device types, and then click Next. The Network Type page opens.
4. Do the following:
   - In the Adapter Type section, select **VMXNET 3**.
   - In the Network Connection section, select an unassigned promiscuous port group.
   - In the Device Status section, make sure that the **Connect at power on** check box is selected.

5. Click **Next** to see a summary.
6. After reviewing the settings, click **Finish**.
7. The Flow Sensor VE Virtual Machine Properties dialog opens, showing the newly defined monitor port.

8. Will the Flow Sensor VE be monitoring another virtual switch/VDS on the ESX server/cluster?
   - If yes, repeat this procedure for the next virtual switch.
   - If no, click **OK** to return to the vSphere Client Home page.

9. Continue with the next chapter, "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

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.

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.

   **Note:** You may need to enable the Full Screen Mode (Ctrl+Alt+Enter) to view the entire screen.

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**.
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 5 and 30 alphanumeric characters in length with no spaces. You also may use the following special 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 virtual appliances?

   - If yes, continue with “Configuring a Virtual Appliance System.”
   - If no, return to “Configure the IP Addresses” on page 41 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 VIRTUAL APPLIANCE

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 2 for the information you will need before proceeding.

Process Overview

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

1. Configuring the Individual Appliances
2. Increasing Memory for the Flow Sensor VE
3. Configuration through the Appliance Admin Interface

Configuring the Individual Appliances

Initial configuration of every appliance is done with the Appliance Setup Tool. The first time you access the appliance the Appliance Setup Tool is displayed. Depending on your system, you should configure the Flow Sensors and Flow Collectors before the UDP Directors, and then, lastly, configure the SMC. When you complete the initial setup for the SMC, 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 2.
To configure an appliance, complete the following steps:

1. In the address field of your browser, type `https://` followed by the IP address of the virtual appliance, and then press `Enter`.

2. The admin login page opens. Type `admin` and `lan411cope` (both are case sensitive), and then click `Login`. Go to step 5.

3. The Welcome page opens. Click `Continue`
4. Review the settings you previously entered, and then click **Next**. The Password Management page opens.
5. In the appropriate fields, type your new admin password, and then click Next. The Host Name and Domain page opens.

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

8. 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"
9. Click **Next**. The Review page opens.

![Review page screenshot]

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

![Notice dialogue screenshot]

11. 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.

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

13. Do you have any other appliances to configure?

   - If yes, return to Step 1 and repeat this procedure for the next appliance. Remember to configure the primary SMC last.
   - If no, go to the next step.

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

### Increasing Memory for the Flow Sensor VE

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** and increase the memory size to 4 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 next 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?
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.

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:
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.
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:
1. On the Appliance Admin interface menu, select **Operations > Restart Appliance**.

![Screenshot of the Appliance Admin interface showing the Operations menu with an arrow pointing to the Restart Appliance option.]

   The confirmation dialog opens.

![Screenshot of the confirmation dialog.]

2. Click **Yes**.
3. After restarting, the Flow Sensor VE will begin collecting data from the VM environment and sending it to the NetFlow collector.

   Congratulations, you have now completely installed and configured the Flow Sensor VE! It should now appear on the SMC Client Enterprise tree under the **Flow Sensors** and **VM Servers** branches. The Flow Sensor will not appear on the SMC Enterprise tree until the Flow Sensor detects traffic and sends data to the Flow Collector, which sends data to the SMC.

   Please see the **SMC Client Online Help** for more information.