UDP Director Virtual Edition
Installation and Configuration Guide
(for Stealthwatch System v6.9.0)
# CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contents</td>
<td>iii</td>
</tr>
<tr>
<td>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 UDP Director VE</td>
<td>1</td>
</tr>
<tr>
<td>Before You Begin</td>
<td>2</td>
</tr>
<tr>
<td>How to Use This Guide</td>
<td>4</td>
</tr>
<tr>
<td>Other Resources</td>
<td>5</td>
</tr>
<tr>
<td>Installing a Virtual Appliance</td>
<td>7</td>
</tr>
<tr>
<td>Overview</td>
<td>7</td>
</tr>
<tr>
<td>Process Overview</td>
<td>7</td>
</tr>
<tr>
<td>Configuring Your Firewall for Communications</td>
<td>8</td>
</tr>
<tr>
<td>Communication Ports</td>
<td>8</td>
</tr>
<tr>
<td>Logging in to the VMware vSphere Client</td>
<td>11</td>
</tr>
<tr>
<td>Adding a Resource Pool</td>
<td>12</td>
</tr>
<tr>
<td>Installing the Virtual Appliance</td>
<td>14</td>
</tr>
<tr>
<td>Configuring the Virtual Environment</td>
<td>23</td>
</tr>
<tr>
<td>Overview</td>
<td>23</td>
</tr>
<tr>
<td>Configure the IP Addresses</td>
<td>23</td>
</tr>
<tr>
<td>Change the Default User Passwords</td>
<td>27</td>
</tr>
<tr>
<td>Changing the sysadmin Password</td>
<td>27</td>
</tr>
<tr>
<td>Changing the root Password</td>
<td>30</td>
</tr>
<tr>
<td>Configuring a Virtual Appliance</td>
<td>33</td>
</tr>
<tr>
<td>Overview</td>
<td>33</td>
</tr>
<tr>
<td>Process Overview</td>
<td>33</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Configuring the Individual Appliances</td>
<td>33</td>
</tr>
<tr>
<td>Configuring the UDP Director from the SMC</td>
<td>38</td>
</tr>
<tr>
<td>Adding a UDP Director</td>
<td>38</td>
</tr>
<tr>
<td>Configuring Forward Rules</td>
<td>39</td>
</tr>
<tr>
<td>Configuration through the Appliance Admin Interface</td>
<td>41</td>
</tr>
<tr>
<td>Log in to the Appliance Administration Interface</td>
<td>42</td>
</tr>
<tr>
<td>Configure the System Time</td>
<td>43</td>
</tr>
<tr>
<td>Configure UDP Director VE Rules</td>
<td>45</td>
</tr>
<tr>
<td>Restart the Virtual Appliance</td>
<td>47</td>
</tr>
</tbody>
</table>
INTRODUCTION

Overview

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

About the UDP Director VE

The UDP Director VE is a virtual appliance that serves as a central collector for flow data generated by flow-enabled devices.

The Stealthwatch UDP Director VE is a high-speed, high-performance UDP packet replicator. The UDP Director VE is very helpful in redistributing NetFlow, sFlow,
syslog, or Simple Network Management Protocol (SNMP) traps to various collectors.

As it receives UDP packets from multiple sources, the UDP Director VE aggregates the information into a single data stream. It then modifies the packets to appear as though they came from the original source, and sends the data to multiple destinations. Network and security administrators define the rules by which aggregated information is collected and distributed, based on source IP, destination IP and destination port.

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. FlowSensor 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. Cisco AnyConnect configuration guides are at the Cisco web site.
Resource Requirements

This section provides the resource requirements for the virtual appliances.

UDP Director VE

The UDP Director VE requires that the VMware server meets the following specifications:

- 4 GB RAM
- 50 GB disk space

Note: Lancope recommends thick provisioning although thin provisioning can be used if disk space is limited.

Information Needed for the vSphere Client Interface

<table>
<thead>
<tr>
<th>Setting</th>
<th>ESX/vSphere Server</th>
<th>UDP Director 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 = 192.168.1.2)</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>UDP Replicator VE</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>(Default = 192.168.1.2)</td>
</tr>
<tr>
<td>Host Name</td>
<td></td>
</tr>
<tr>
<td>Network Domain Name</td>
<td></td>
</tr>
<tr>
<td>NTP Server IP Address(es)</td>
<td></td>
</tr>
<tr>
<td>DNS Server IP Address(es)</td>
<td></td>
</tr>
</tbody>
</table>
### Information Needed for the vSphere Client Interface

#### 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>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>
</tbody>
</table>
Other Resources

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

Related Documents

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

You can also open the Documentation Library from one of the following links:

- On the SMC Web App interface, click the Help button and select Documentation Library,
- In the main menu of the SMC client interface, click Help > Documentation.
- In the main menu of the Appliance Admin interface, click Help > Documentation Library.

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

Lancope Blog

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

Lancope Resources & Tools for Advanced Cybersecurity

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

Contacting Support

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

© 2016 Cisco Systems, Inc. All Rights Reserved.
• Contact your local Cisco partner.
• Call +1 800-838-6574.
• Submit a case using the Support form on the Lancope Customer Community web site (https://lancope.force.com/Customer/CustomerCommLogin)

Document Feedback

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

Overview

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

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

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

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

Process Overview

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

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

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

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

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

Communication Ports

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

<table>
<thead>
<tr>
<th>From (Client)</th>
<th>To (Server)</th>
<th>Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin User PC</td>
<td>All appliances</td>
<td>TCP/443</td>
<td>HTTPS</td>
</tr>
<tr>
<td>All appliances</td>
<td>Network time source</td>
<td>UDP/123</td>
<td>NTP</td>
</tr>
<tr>
<td>Active Directory</td>
<td>SMC</td>
<td>TCP/389, UDP/389</td>
<td>LDAP</td>
</tr>
<tr>
<td>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>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>FlowSensor</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>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 Collector</td>
<td>TCP/443</td>
<td>HTTPS</td>
</tr>
<tr>
<td>SMC</td>
<td>FlowSensor</td>
<td>TCP/443</td>
<td>HTTPS</td>
</tr>
<tr>
<td>SMC</td>
<td>Identity</td>
<td>TCP/2393</td>
<td>SSL</td>
</tr>
<tr>
<td>SMC</td>
<td>Flow Exporters</td>
<td>UDP/161</td>
<td>SNMP</td>
</tr>
<tr>
<td>SMC</td>
<td>Endpoint Concentrator</td>
<td>UDP.2055</td>
<td>HTTPS</td>
</tr>
<tr>
<td>User PC</td>
<td>SMC</td>
<td>TCP/443</td>
<td>HTTPS</td>
</tr>
</tbody>
</table>

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

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

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

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

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

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

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

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

---

### Adding a Resource Pool

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

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

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

1. In the Inventory tree on the left, right-click the ESX server IP address, and then select **New Resource Pool** from the popup menu or on the Web client select **All vCenter Actions > New Resources Pool**.
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.
   - Change the Limit field to at least 4 GB (8 GB recommended).
   - Click the Unlimited checkbox to clear it.
7. Click **OK**. The resource pool appears beneath the ESX server on the Inventory tree.

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

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

## Installing the Virtual Appliance

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

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

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.


15. When the deployment is completed, click Close to close the progress dialog. The virtual appliance appears in the Inventory tree.
16. Have you completed all of the procedures in this chapter for all of the UDP Directors?

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

Overview

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

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

Configure the IP Addresses

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

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

   **Note:** If the virtual machine does not power on and you receive an error message about insufficient available memory, do one of the following:

   - Increase the memory reservation limit for the appliance and its resource pool.
   - Increase the available resources on the system where the appliance is installed.
   - Decrease the memory allocation and reservation to 4 GB.

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

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

   **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**.

   ![System Configuration Menu](image)

**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.

![Prompt for Current Password](image)

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

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

**Notes:**

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

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

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

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

To change the root password, complete the following steps:

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

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

   A prompt for the root password appears.

3. Type the current root password, **lan1cope**, and then press **Enter**. The root shell prompt appears.
4. Type **SystemConfig** (case-sensitive), and then press **Enter**.

This returns you to the System Configuration menu so that you can change the root password.

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

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

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

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

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

10. Have you completed all of the procedures in this chapter for all of the virtual appliances?

   - If yes, continue with “**Configuring a Virtual Appliance System**.”
   - If no, return to “Configure the IP Addresses” on page 23 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. 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 FlowSensors 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.

Note: Your screens may look slightly different from the ones presented here depending on your environment.
To configure an appliance, complete the following steps:

1. In the address field of your browser, type `https://` followed by the IP address of the 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

3. The Welcome page opens. Click **Continue**

The Management Network Interface page opens.
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.
10. Review your settings, and then click **Apply**. The confirmation dialogue opens.

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. Are you managing the UDP Director from the SMC?
   - If yes, continue with the next section, *Configuring the UDP Director from the SMC*
   - If no, go to “*Configuration through the Appliance Admin Interface*” on page 41.”

### Configuring the UDP Director from the SMC

If you have UDP Directors in your Stealthwatch System, then you can configure them from the SMC Web App so that the SMC manages the UDP Directors. For managing from the UDP Director itself, go to See "*Configuring a Virtual Appliance*"

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

### Adding a UDP Director

To add a UDP Director, complete the following steps:

![UDP Director Configuration](image)
After adding a UDP Director, you can configure forward rules for it.

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

2. Click **Add New Rule**.

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

- Use the syntax [IP address][Port Number], as shown in the examples below.
- You can use Classless Inter-Domain Routing (CIDR) notation to enter a range of IP addresses.
- You can type "All" to accept data from any source IP address on this port.
- You can add Source IP Address:Port combinations within a rule by adding them to a new line.

Examples:

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

5. In the Destination IP Address field, enter the IP address of the device receiving data from the UDP Director.
6. In the Destination Port Number field, enter the port number for the receiving device.
7. Click Save. The new rule is added to the table on Forwarding Rules page.
8. Do you want to sync the changes?
   a. If yes, click the Sync button at the top of the page. The new rule is saved.
   b. If no, click the Discard Edits button at the top of the page. When the Configuration dialogue appears, click Yes.

8. Repeat the procedure to add forwarding rules as needed.
9. Continue with the next section, "Configuration through the Appliance Admin Interface."

Note: If you want to have a secondary UDP Director, you must have added it with at least one forwarding rule. You first need to configure the Primary UDP Director and then repeat the configuration on the Secondary one. For the instructions for configuring HA appliances, go to "Configuring a Virtual Appliance" on page 33

Configuration through the Appliance Admin Interface

This section provides the following procedures to complete the configuration of a virtual appliance using its Appliance Admin interface:
1. Log in to the Appliance Administration Interface
2. Configure the System Time
3. Configure UDP Director VE Rules
4. 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 reopen 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.

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

Configure the System Time

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

**CAUTION!** Use the same NTP server used for the Flow Collectors and other devices that feed information to the SMC.

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

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

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, “Configure UDP Director VE Rules.”

**Configure UDP Director VE Rules**

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

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

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

1. On the Admin Web interface menu, click **Configuration > Forwarding Rules**.
The Forwarding Rules page opens.

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

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

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

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

   A new line appears where you can enter the settings. Repeat this step until you have entered all devices for this UDP Director.
8. When finished, click Apply. The UDP Director Configuration screen refreshes and the system updates the configuration file. Any errors appear at the top of the screen.
9. Continue with the next section, Configuring a Virtual Appliance

**Restart the Virtual Appliance**

To restart the virtual appliance, complete the following steps:

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

   ![Restart Appliance Menu](https://example.com/restart.png)

   The confirmation dialog opens.
2. Click **Yes**.

3. After restarting, the UDP Director VE will begin collecting data and sending it to the configured destinations.