



UDP Director Virtual Edition

(also known as FlowReplicator VE)

Installation and Configuration Guide

(for StealthWatch System v6.7.0)

Installation and Configuration Guide: UDP Director VE v6.7.0

© 2015 Lancope, Inc. All rights reserved.

Document Date: March 23, 2015

Trademarks

Lancope, StealthWatch, and other trademarks are registered or unregistered trademarks of Lancope, Inc. Cisco, Cisco Identity Services Engine, and Cisco TrustSec are trademarks or registered trademarks of Cisco Systems, Inc., and/or affiliates in the U.S. and other countries. All other trademarks are properties of their respective owners.

CONTENTS

1-INTRODUCTION	5
Overview	5
Audience	5
Before You Begin	6
Downloading the VE Software	6
Resource Requirements	6
UDP Director VE (also known as FlowReplicator VE)	6
Information Needed for the vSphere Client Interface	7
Information Needed for the Appliance Admin Interface	7
About the UDP Director VE	7
How to Use This Guide	8
Documentation Icons	9
Abbreviations	9
Other Resources	10
2-INSTALLING A VIRTUAL APPLIANCE	13
Overview	13
Process Overview	14
Configuring Your Firewall for Communications	15
Communication Ports	15
Adding a Resource Pool	19
Installing the Virtual Appliance	22
3-CONFIGURING THE VIRTUAL ENVIRONMENT	31
Overview	31
Configure the IP Addresses	32
Change the Default User Passwords	37
Changing the sysadmin Password	37
Changing the root Password	39
4-CONFIGURING A VIRTUAL APPLIANCE	43
Overview	43
Process Overview	43
Configuring the Individual Appliances	44
Configuration through the Appliance Admin Interface	50
Log in to the Appliance Administration Interface	50



Configure the System Time	51
Change the Admin Password	53
Configure UDP Director VE Rules	55
Restart the Virtual Appliance	58



INTRODUCTION

OVERVIEW

This is an installation and configuration guide for the UDP Director VE (also known as FlowReplicator VE) in a network using vSphere Client v4.x or v5.x. Beginning with v6.6.0, the FlowReplicator VE is called the UDP Director VE.



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 Lancope Customer Support, if needed. This chapter includes the following sections:

- ▶ Audience
- ▶ Before You Begin
- ▶ About the UDP Director VE
- ▶ How to Use This Guide

Audience

The primary audience for this guide is administrators who need to install and configure StealthWatch UDP Director VE (also known as FlowReplicator VE) appliances. This guide assumes the audience has a basic familiarity with VMware software.



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. UDP Director VE (also known as FlowReplicator VE)
2. FlowSensor VE
3. FlowCollector VE
4. SMC VE

If you do not follow this recommended order, when you set up the StealthWatch system, the SMC VE 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.

Resource Requirements

This section provides the resource requirements for the virtual appliances.

UDP Director VE (also known as FlowReplicator VE)

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

- ▶ 4 GB RAM
- ▶ 50 GB disk space



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

Information Needed for the vSphere Client Interface

Setting	ESX/vSphere Server	UDP Director VE
Login User Name		
Login Password		
IP Address		(Default = 192.168.1.2)
Netmask IP Address		(Default = 255.255.255.0)
Gateway IP Address		(Default = 192.168.1.1)

Information Needed for the Appliance Admin Interface

Setting	UDP Replicator VE
IP Address	(Default = 192.168.1.2)
Host Name	
Network Domain Name	
NTP Server IP Address(es)	
DNS Server IP Address(es)	



Note:

The password must be between 5 and 30 alphanumeric characters in length with no spaces. You also may use the following special characters:
`$.~!@#%_=?:,{}()`

About the UDP Director VE

Using the same technology as the FlowReplicator appliance, the UDP Director VE (also known as FlowReplicator VE) is a virtual appliance that serves as a central collector for flow data generated by flow-enabled devices.

The StealthWatch FlowReplicator is a high-speed, high-performance UDP packet replicator. The FlowReplicator 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 FlowReplicator 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.






How to Use This Guide

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

Chapter	Description
Chapter 2, "Installing a Virtual Appliance."	How to install VE appliances on an ESX server using vSphere Client v4.x or v5.x
Chapter 3, "Configuring the Virtual Environment."	How to set up the virtual environment for the appliances
Chapter 4, "Configuring a Virtual Appliance."	How to configure appliances to begin processing traffic data

Documentation Icons

This guide uses the following documentation icons.

Icon	Meaning	Includes Information...
	Tip	Such as a shortcut or an easier way of performing a certain task.
	Note	You may find useful as you use this document or the StealthWatch System.
	Important	You must observe to prevent significant consequences, such as the malfunction of software.
	Caution	You must observe to prevent loss of data or damage to hardware.
	Warning	You must observe to prevent risk of personal injury.

Abbreviations

The following abbreviations appear in this guide:

Abbreviations	Definition
DNS	Domain Name System (Service or Server)
dvPort	Distributed Virtual Port
ESX	Enterprise Server X
GB	Gigabyte
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IT	Information Technology
MTU	Maximum Transmission Unit
NTP	Network Time Protocol
OVF	Open Virtualization Format
SMC	StealthWatch Management Console

Abbreviations	Definition
TB	Terabyte
UUID	Universally Unique Identifier
VDS	vNetwork Distributed Switch
VE	Virtual Edition
VLAN	Virtual Local Area Network
VM	Virtual Machine

Other Resources

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

Related Documents

Please refer to your StealthWatch Documentation CD for information about StealthWatch appliances and their installation and configuration.

Additional information is available in the Lancope Community Web site (community.lancope.com/). If you do not have login access to the web site, send an email requesting access to support@lancope.com.

NetFlow Ninjas Blog

Lancope's *NetFlow Ninjas* 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.

StealthWatch Video Library

The StealthWatch online video library at <http://www.lancope.com/resource-center/videos/> showcases the benefits of StealthWatch for network performance and security management.

Contacting Support

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

- ▶ Contact your local Lancope partner.
- ▶ Send an email requesting assistance to support@lancope.com.
- ▶ Call +1 800-838-6574.
- ▶ Submit a case using the Support form on the Lancope Customer Community web site (<https://community.lancope.com>)

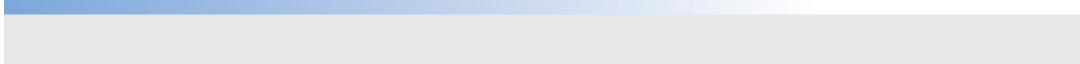
You will need to provide the following information:

- ▶ Your name
- ▶ Your company name
- ▶ Location

Document Feedback

If you have comments about this document, please contact Lancope 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 v6.5x Hardware Installation Guide*.

This chapter describes how to install the virtual appliances using VMware vSphere Client v4.x or v5.x.



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. Adding a Resource Pool
3. 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 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
- ▶ UDP 53
- ▶ UDP 123
- ▶ UDP 161
- ▶ UDP 162
- ▶ UDP389
- ▶ UDP 514
- ▶ UDP 2055
- ▶ UDP 3514
- ▶ UDP 6343

Communication Ports

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

From (Client)	To (Server)	Port	Protocol
Admin User PC	All appliances	TCP/443	HTTPS
All appliances	Network time source	UDP/123	NTP
Active Directory	SMC	TCP/389, UDP/389	LDAP
Cisco ISE	SMC	TCP/443	HTTPS
- continued -			



From (Client)	To (Server)	Port	Protocol
Cisco ISE	SMC	UDP/3514	SYSLOG
External log sources	SMC	UDP/514	SYSLOG
FlowCollector	SMC	TCP/443	HTTPS
SLIC	SMC	TCP/443 or proxied connection	HTTPS
UDP Director (also known as FlowReplicator)	FlowCollector - sFlow	UDP/6343	sFlow
UDP Director (also known as FlowReplicator)	FlowCollector - NetFlow	UDP/2055*	NetFlow
UDP Director (also known as FlowReplicator)	3 rd Party event management systems	UDP/514	SYSLOG
FlowSensor	SMC	TCP/443	HTTPS
FlowSensor	FlowCollector - NetFlow	UDP/2055	NetFlow
IDentity	SMC	TCP/2393	SSL
NetFlow Exporters	FlowCollector - NetFlow	UDP/2055*	NetFlow
sFlow Exporters	FlowCollector - sFlow	UDP/6343*	sFlow
SMC	Cisco ISE	TCP/443	HTTPS
SMC	DNS	UDP/53	DNS
SMC	FlowCollector	TCP/443	HTTPS
SMC	FlowSensor	TCP/443	HTTPS
SMC	IDentity	TCP/2393	SSL
SMC	Flow Exporters	UDP/161	SNMP
User PC	SMC	TCP/443	HTTPS

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

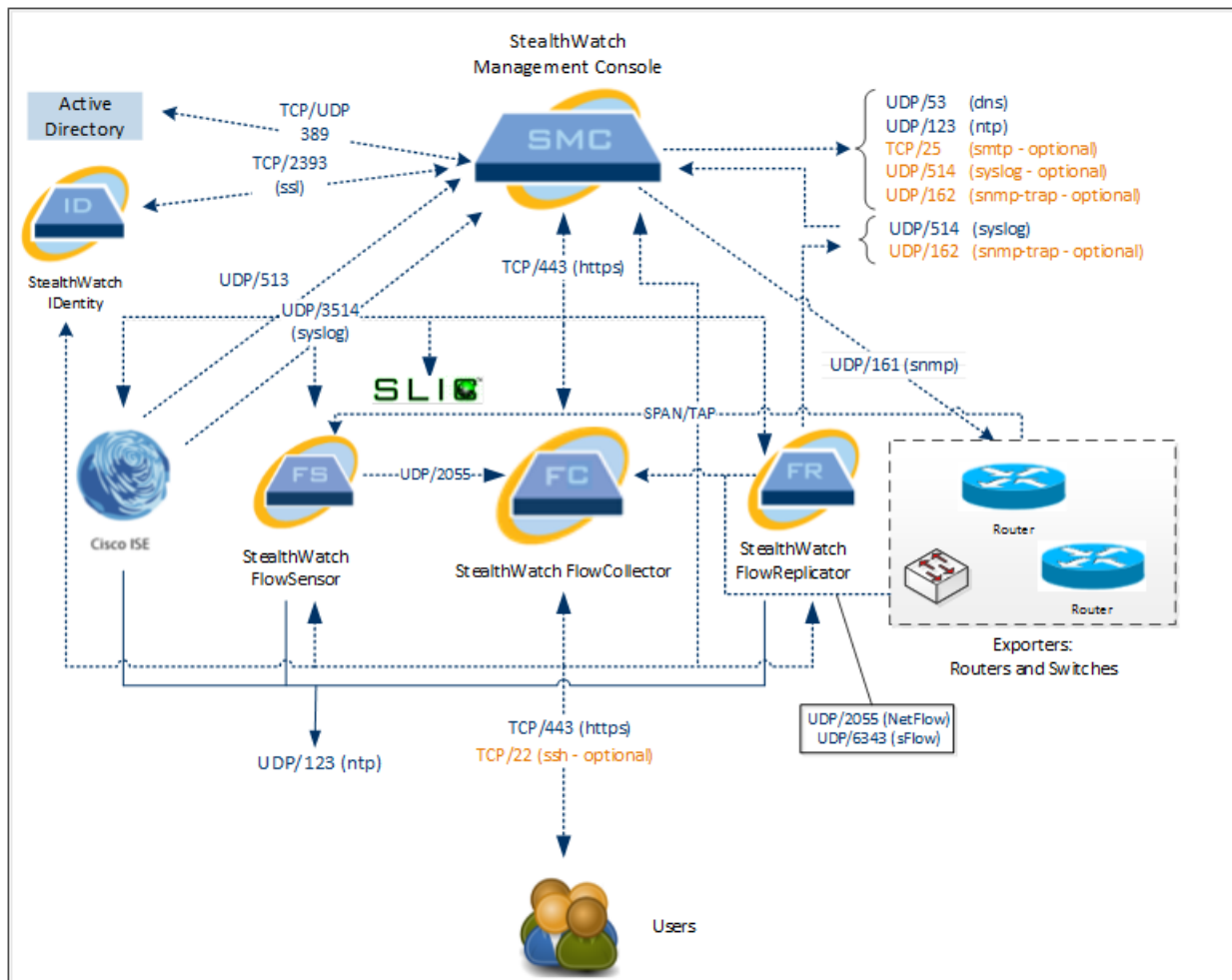
The following table is for optional configurations determined by your network needs:

From (Client)	To (Server)	Port	Protocol
All appliances	User PC	TCP/22	SSH



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

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:

The screen images are for VMWare v5.0 and may appear slightly different from your screens, but the commands are the same.

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.

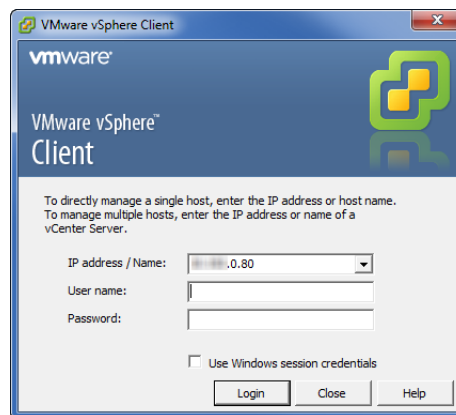


Note:

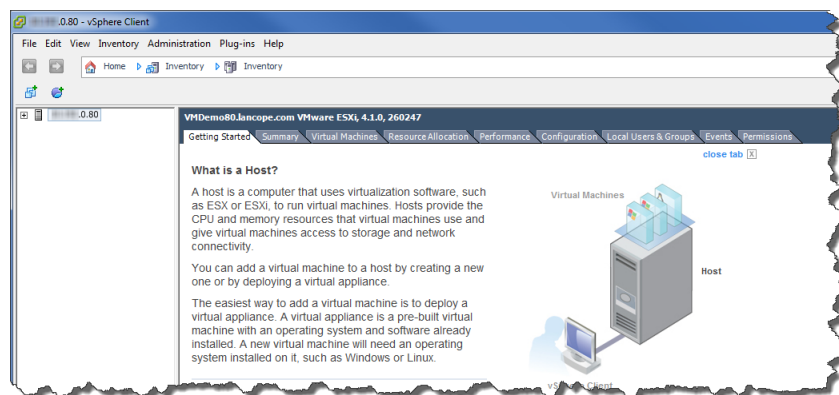
If desired, you can use an existing resource pool for a virtual appliance. However, you should examine this procedure to make sure the existing resource pool has enough resources allocated to it for a virtual appliance to operate properly.

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

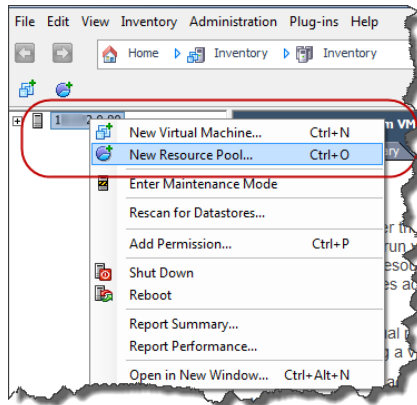
1. Launch the VMware vSphere client software. The Login dialog opens.



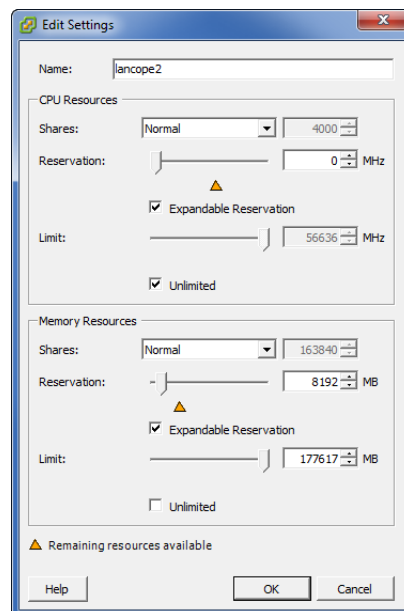
2. Enter the IP address of the ESX server and your login credentials, and then click **Login**. The Getting Started page opens.



3. In the Inventory tree on the left, right-click the ESX server IP address, and then select **New Resource Pool** from the popup menu.



The Create Resource Pool dialog opens.



4. In the **Name** field, type the name you want to use to identify this resource group.
5. Do not change any of the settings in the CPU Resources section.
6. 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 6.
 - ▶ Change the Limit field to at least **4 GB (8 GB recommended)**.

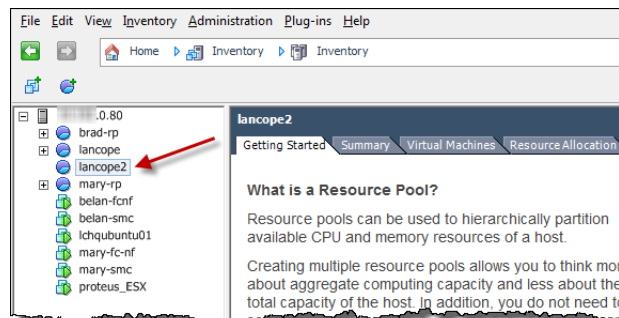
- ▶ Click the **Unlimited** checkbox to clear it.



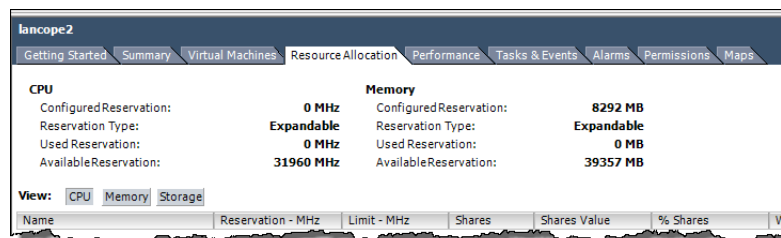
CAUTION:

Less than 4 GB of memory is not supported. If less than 4 GB is allocated, a Low Memory alarm will be triggered, and no flows will be stored in the database.

- Click **OK**. The resource pool appears beneath the ESX server on the Inventory tree.



- Select the resource pool, and then click the **Resource Allocation** tab to review the CPU and memory resource allocations.



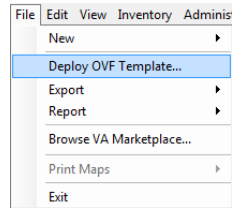
- Continue with the next section, “Installing the Virtual Appliance.”



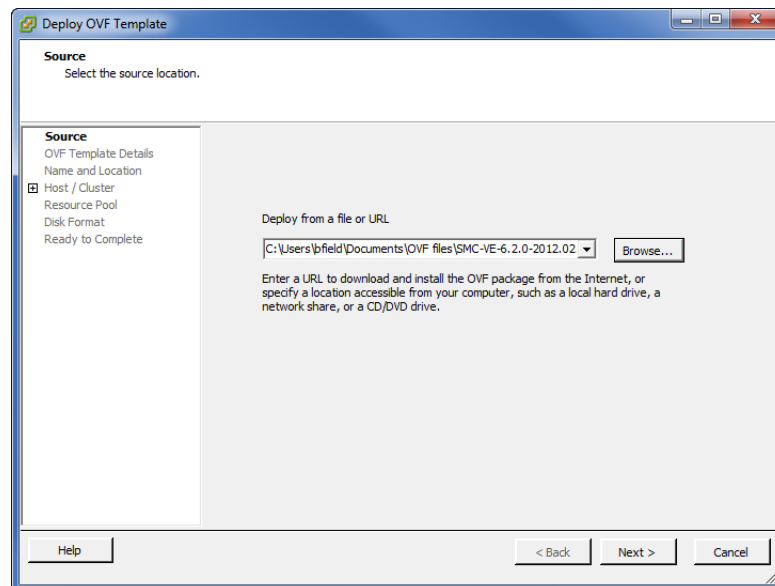
INSTALLING THE VIRTUAL APPLIANCE

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**.

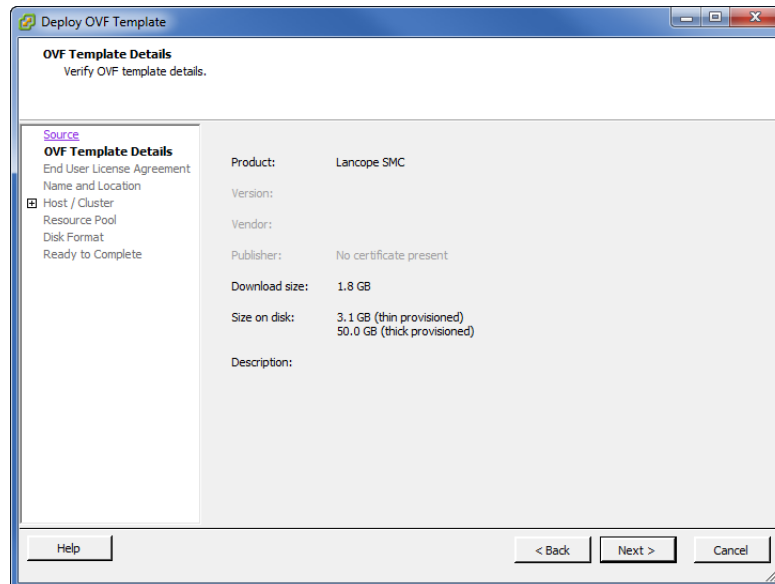


The Deploy OVF Template wizard opens.

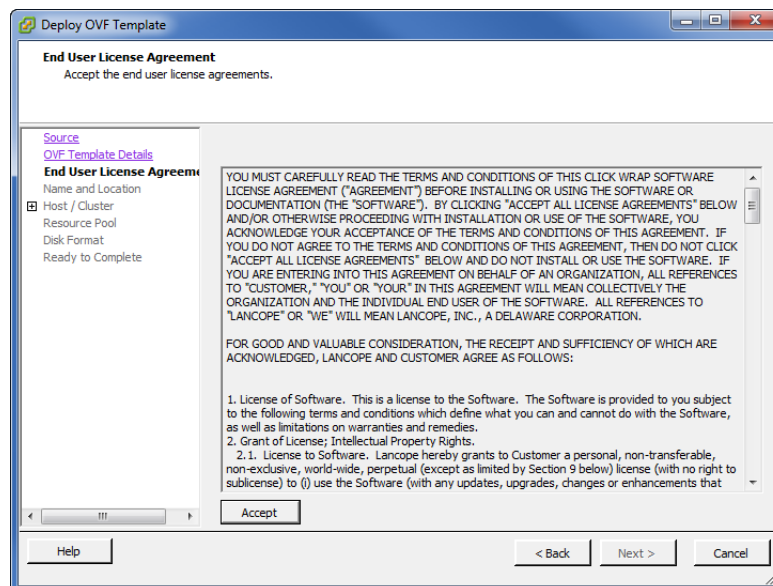


3. Click **Browse**, and then navigate to select the virtual appliance OVF file.

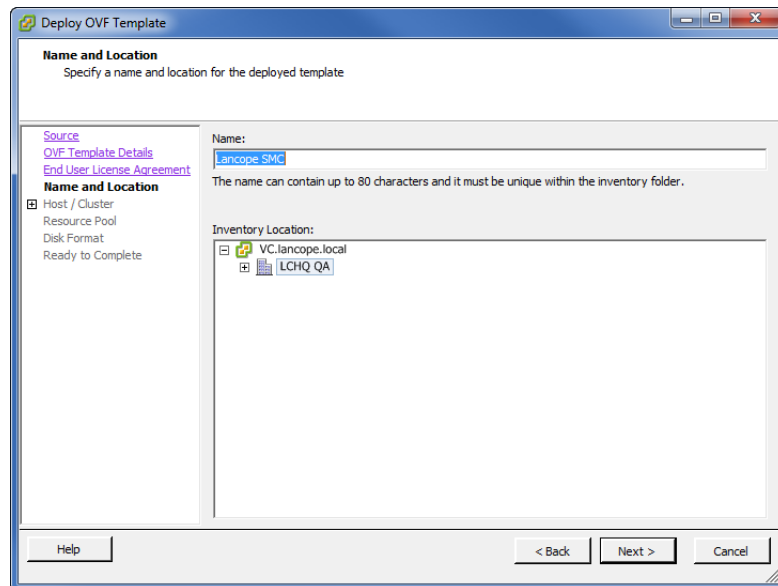
4. Click **Next** to display the OVF Template Details page.



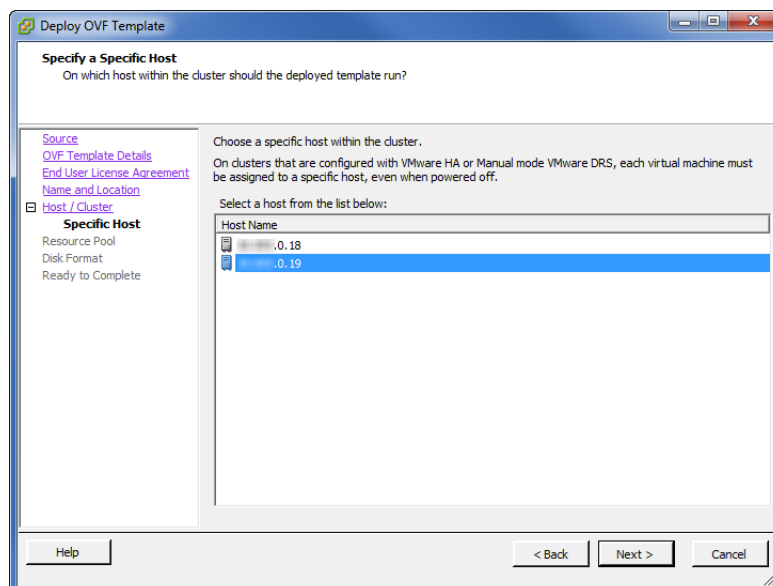
5. Click **Next**. The End User License Agreement opens.



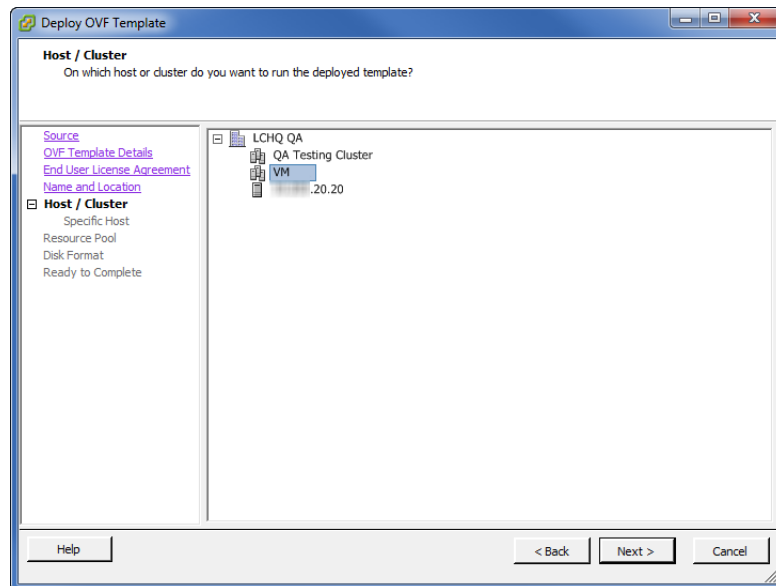
6. After reviewing the information, click **Accept**, and then click **Next**. The Name and Location page opens.



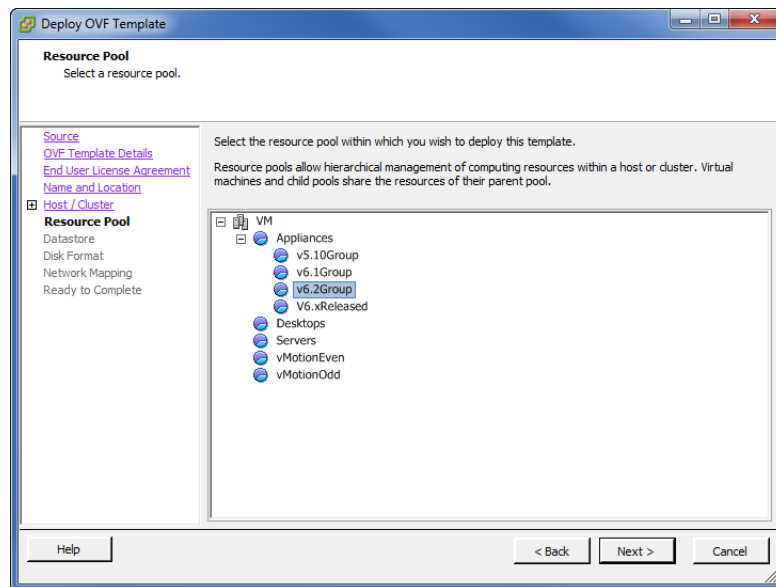
7. If desired, change the name for the virtual appliance as it will appear in the Inventory tree, and then click **Next**.
 - a. If the Specify a Specific Host page opens, select the host or cluster where the virtual appliance will reside.



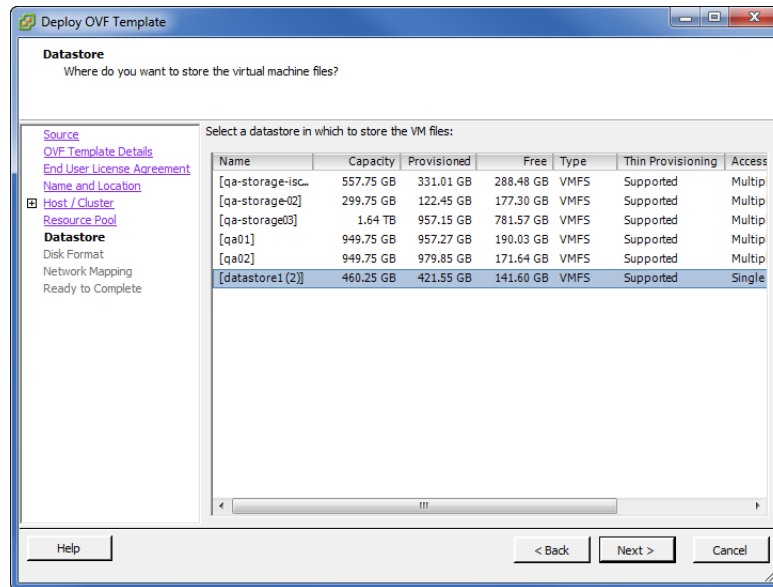
- b. If the Host/Cluster page opens, select the host or cluster where the appliance will reside.



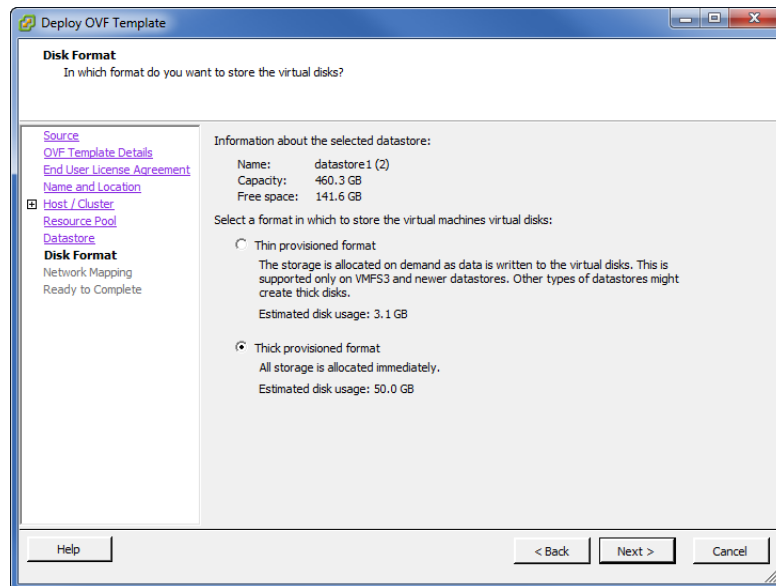
8. Click **Next**. The Resource Pool page opens.



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.
10. On the Datastore page, select where you want to store the virtual appliance, and then click **Next**.



The Disk Format page opens.

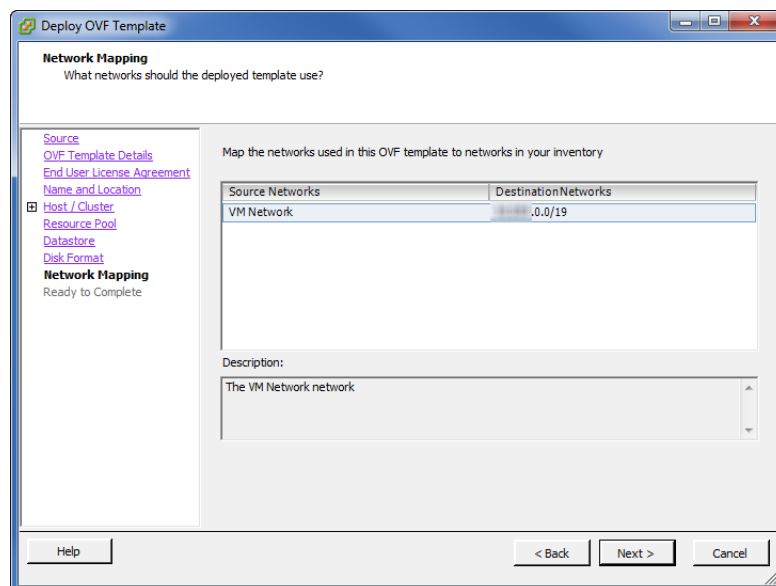


Note:

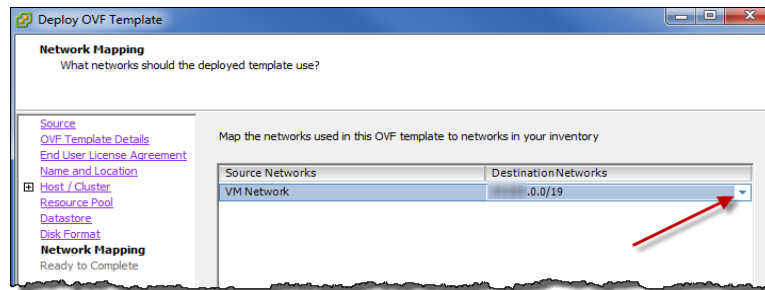


The vSphere Client v5 has two thick-provisioned formats: Lazy Zeroed and Eager Zeroed. Choose the one that best suits your disk storage needs. Use the Thin Provision format only if your disk space is limited. For further information, refer to your VMware documentation.

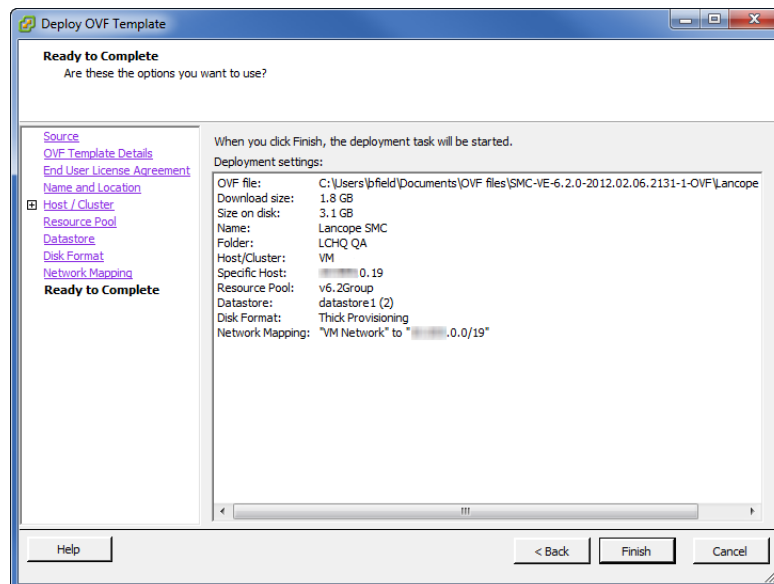
- On the Disk Format page, select **Thick provisioned format**, and then click **Next**. The Network Mapping page opens.



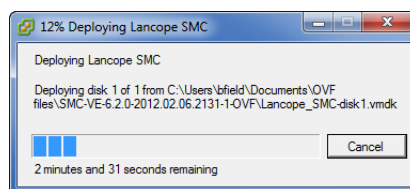
- From the Destination Networks drop-down list, select a virtual appliance management port.



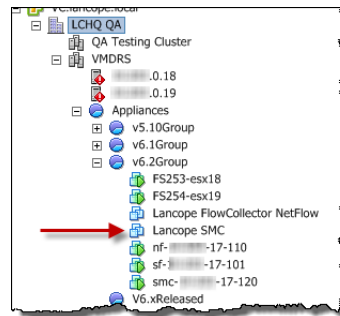
- Click **Next**. The Ready to Complete page opens with a summary of the settings.



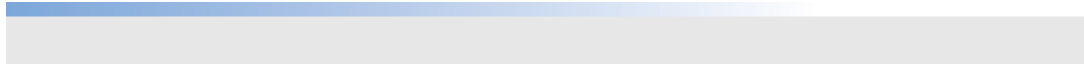
- After reviewing the settings, click **Finish**. A progress dialog opens.



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



16. Have you completed all of the procedures in this chapter for all of the FlowReplicators?
 - ▶ If yes, continue with Chapter 3, “Configuring the Virtual Environment.”
 - ▶ If no, return to “Adding a Resource Pool” on page 19 and repeat all of the procedures in this chapter for the next virtual appliance. Then go to “Configuring the Virtual Environment” on page 31.



3

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:

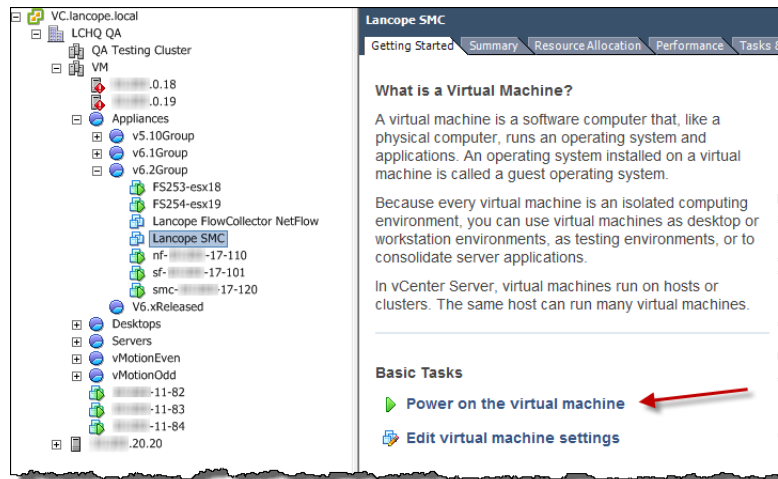
1. Configure the IP Addresses
2. Change the Default User Passwords



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:



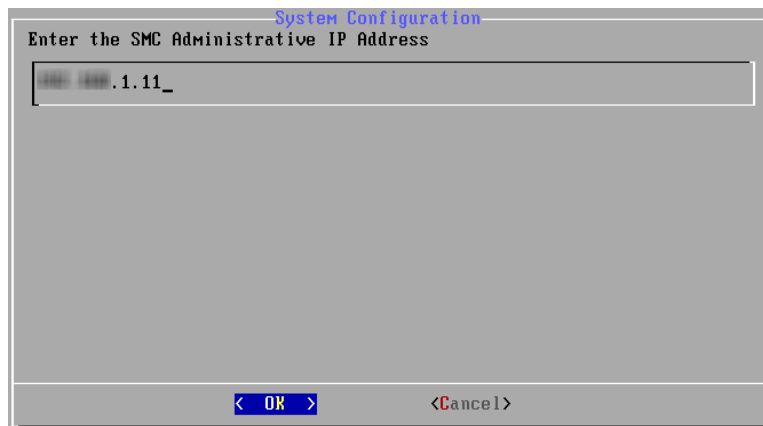
- ▶ Increase the memory reservation limit for the appliance and its resource pool.
- ▶ Increase the available resources on the system where the appliance is installed.
- ▶ Decrease the memory allocation and reservation to 4 GB.

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 6.



- Click the **Console** tab. Allow the virtual appliance to finish booting up. The virtual appliance Administrative IP Address page opens.

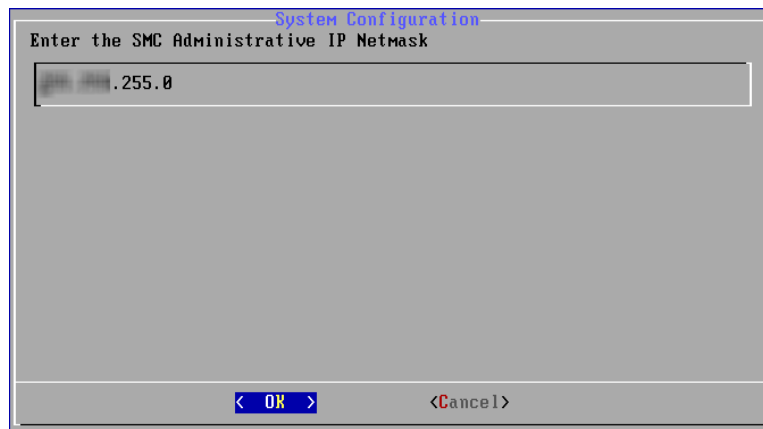


The screenshot shows a dialog box titled "System Configuration" with the prompt "Enter the SMC Administrative IP Address". A text input field contains ".1.11_". At the bottom, there are two buttons: "< OK >" and "<Cancel>".

**Note:**

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

- Click on the page, and then enter the IP address for the virtual appliance.
- Select **OK**, and then press **Enter**. The IP Netmask page opens with the default network mask IP address.

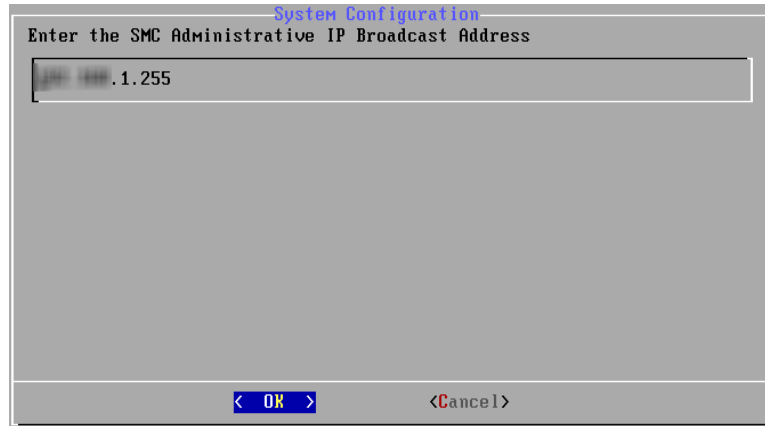


The screenshot shows a dialog box titled "System Configuration" with the prompt "Enter the SMC Administrative IP Netmask". A text input field contains ".255.0". At the bottom, there are two buttons: "< OK >" and "<Cancel>".

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



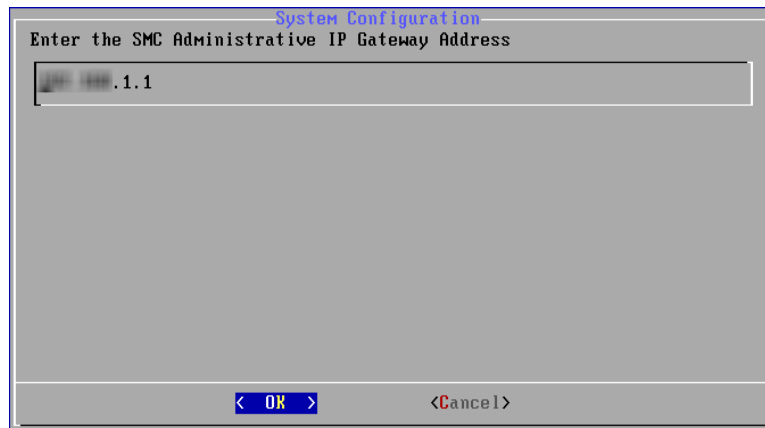
The IP Broadcast Address page opens with the default broadcast IP address.



The screenshot shows a dialog box titled "System Configuration" with the subtitle "Enter the SMC Administrative IP Broadcast Address". A text input field contains the default value "192.168.1.255". At the bottom of the dialog, there are two buttons: "< OK >" and "<Cancel >".

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

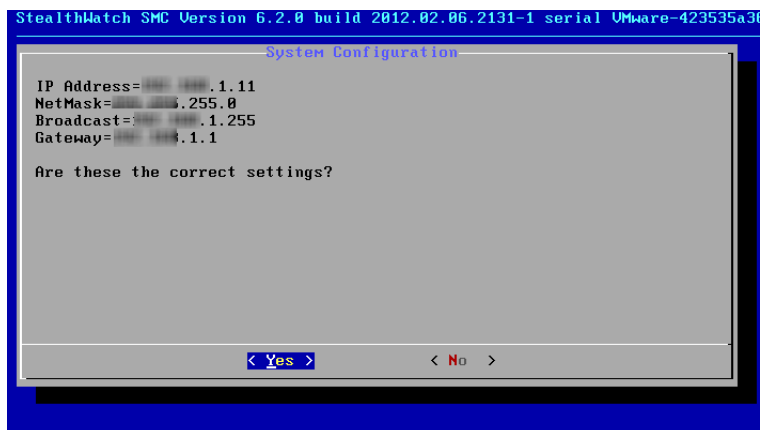
The Gateway Address page opens with the default gateway server IP address.



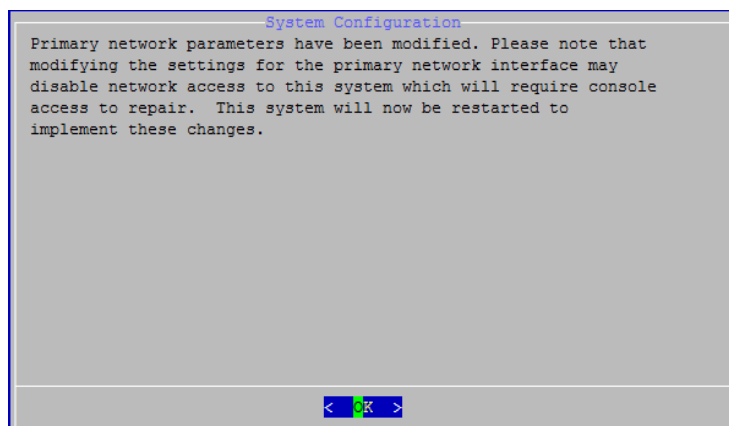
The screenshot shows a dialog box titled "System Configuration" with the subtitle "Enter the SMC Administrative IP Gateway Address". A text input field contains the default value "192.168.1.1". At the bottom of the dialog, there are two buttons: "< OK >" and "<Cancel >".

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 are correct?
 - ▶ If yes, go to step 11.
 - ▶ 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. Go to “Change the Default User Passwords,” next in this chapter.
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.

```
Setting up networking...
INIT: Entering runlevel: 2

Welcome to StealthWatch SMC Version 6.2.8
SMC-01 login: _
```

15. Press **Ctrl + Alt** to exit the console.
16. Go to “Change the Default User Passwords,” next in this chapter.



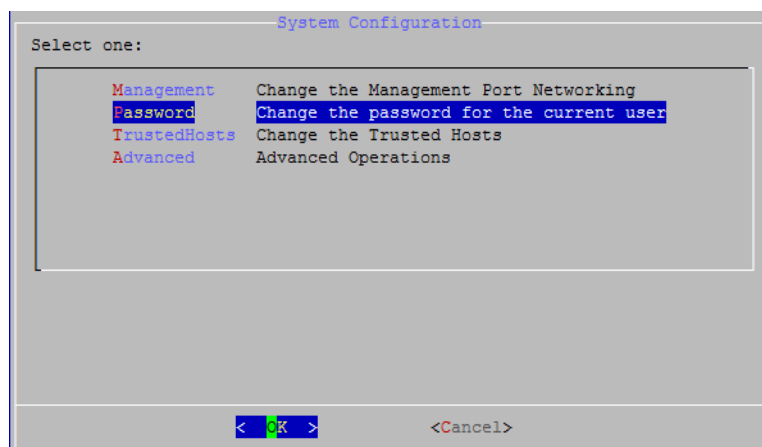
CHANGE THE DEFAULT USER PASSWORDS

To ensure that your network is secure, you should 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. 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**.



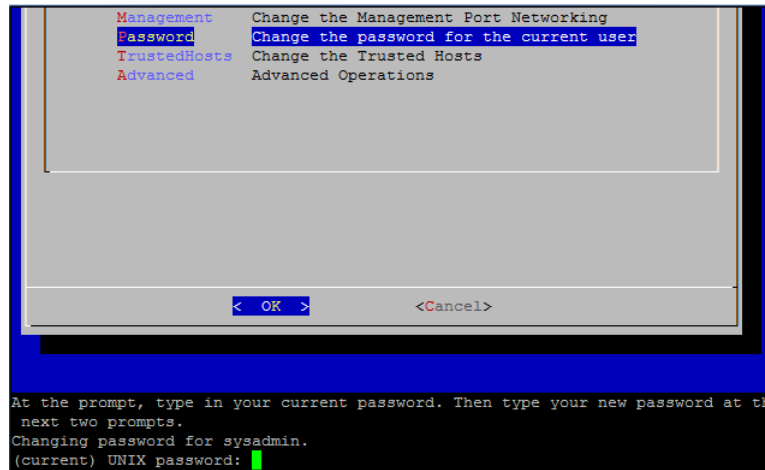
Important:



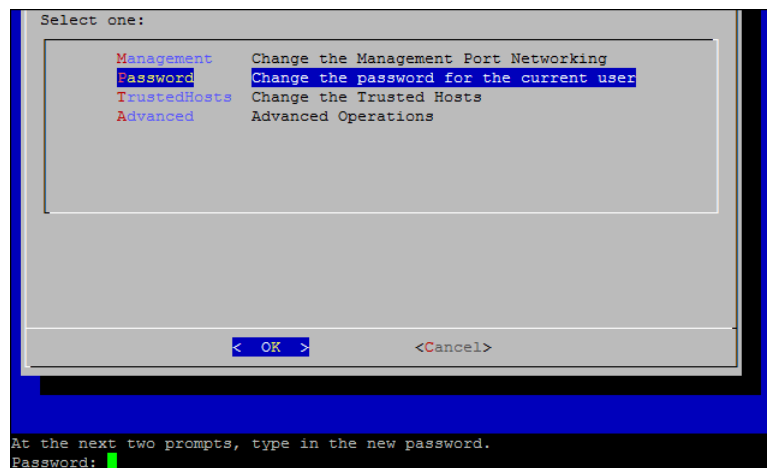
If you change the trusted hosts list from the defaults, you must make sure each StealthWatch appliance is included in the trusted host list for every other StealthWatch appliance in your deployment. Otherwise, the appliances will not be able to communicate with each other.



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**.

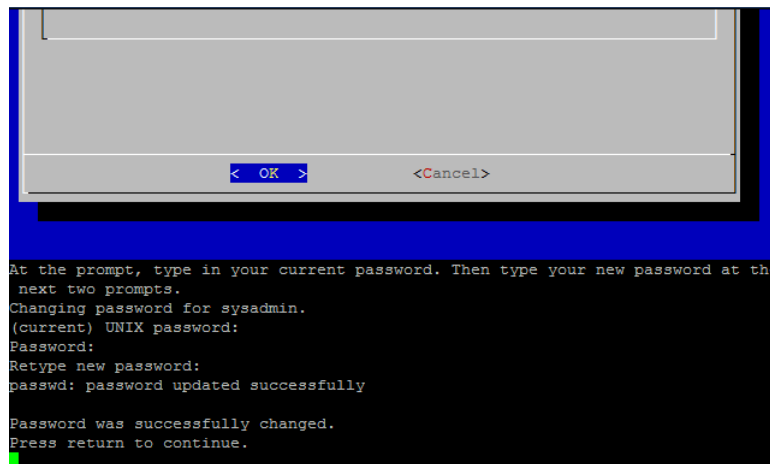
Note:

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.

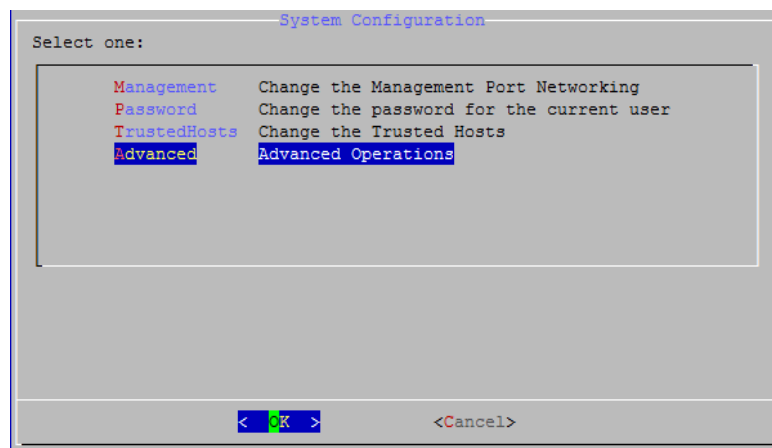


6. Press **Enter** to return to the System Configuration Console menu.
7. Continue with the next section, “Changing the root Password.”

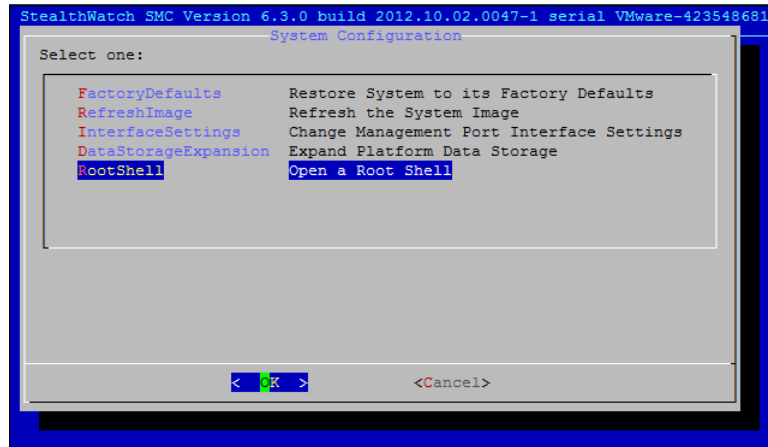
Changing the root Password

To change the root password, complete the following steps:

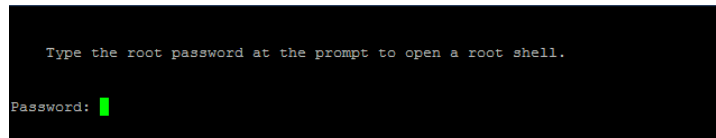
1. On the System Configuration Console menu, select **Advanced**, and then press **Enter**. The Advanced menu opens.



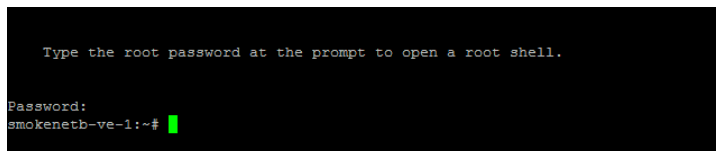
2. On the **Advanced** menu, select **RootShell**, and then press **Enter**.



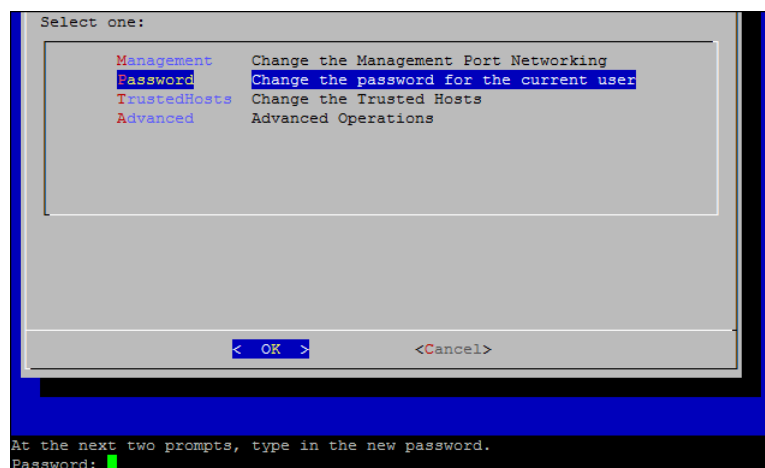
A prompt for the root password appears.



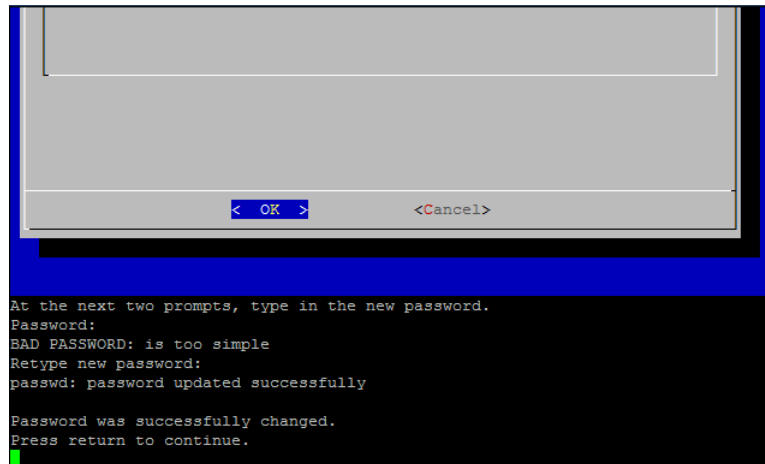
3. Type the current root password, **lan1cope**, and then press **Enter**. The root shell prompt appears.



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.



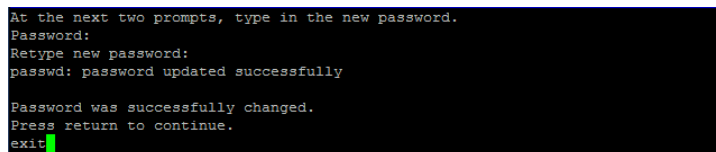
6. Type the new root password, and then press **Enter**. A second prompt appears below the menu.



```
At the next two prompts, type in the new password.
Password:
BAD PASSWORD: is too simple
Retype new password:
passwd: password updated successfully

Password was successfully changed.
Press return to continue.
```

7. Retype the new root password, and then press **Enter**.



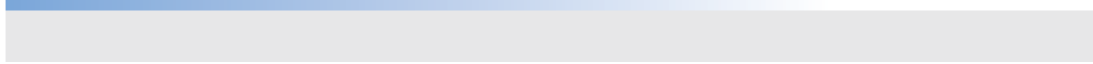
```
At the next two prompts, type in the new password.
Password:
Retype new password:
passwd: password updated successfully

Password was successfully changed.
Press return to continue.
exit
```

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.”
 - ▶ If no, return to “Configure the IP Addresses” on page 32 and repeat all of the procedures in this chapter for the next virtual appliance. Then, go to the “Configuring a Virtual Appliance” on page 43.





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 [page 6](#) 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 FlowCollectors before the UDP Directors (also known as FlowReplicators), 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 “Before You Begin” on page 6.

**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 case sensitive), and then click **Login**. Go to step 4.

STEALTH WATCH[®]
By Lancope
FlowCollector for NetFlow VE
6.6.0

Username:

Password:

Login >>

3. For the SMC VE, the landing page opens.

STEALTH WATCH[®]
By Lancope

Vision to secure,
Intelligence to protect™

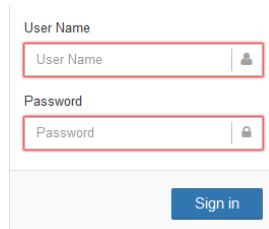
Sign In

User Name

Password

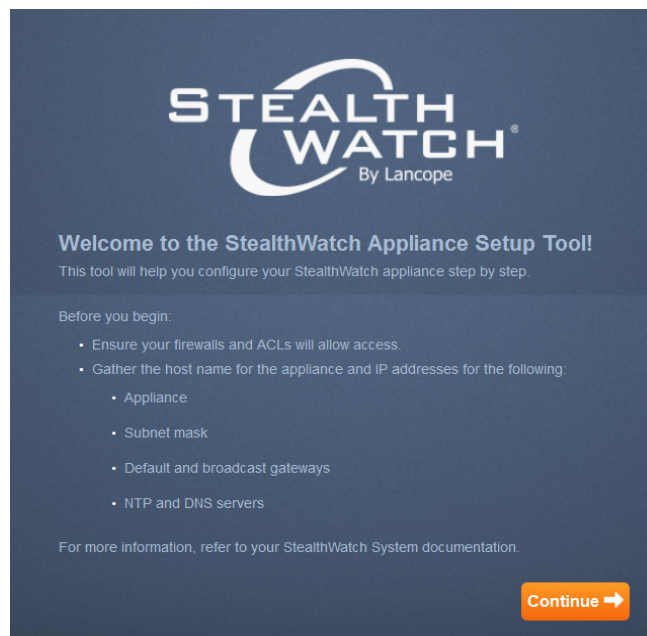
Sign in

To log in, do the following:

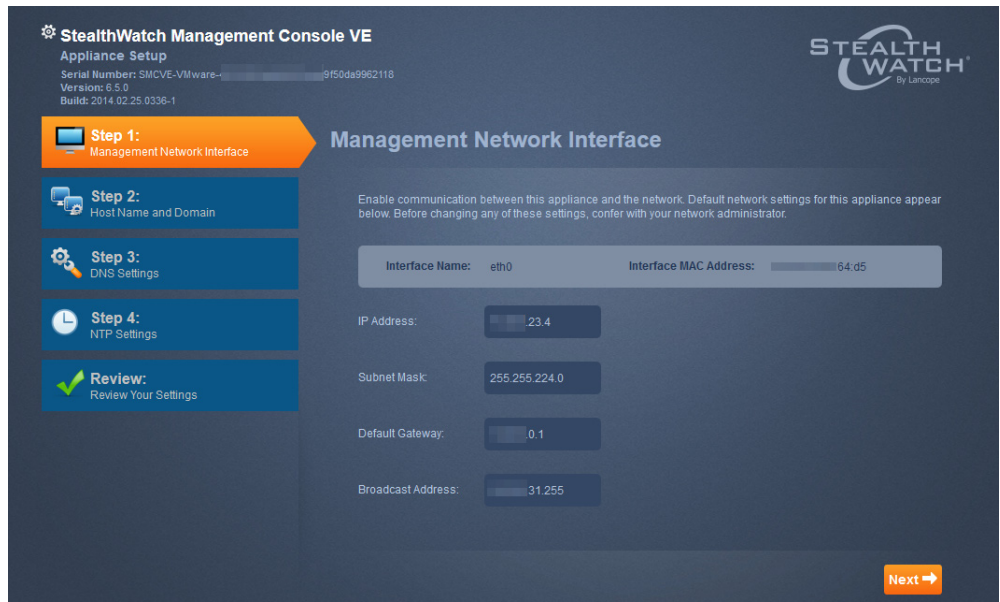


The login form consists of two input fields and a button. The first field is labeled 'User Name' and contains the text 'User Name' with a user icon. The second field is labeled 'Password' and contains the text 'Password' with a lock icon. Below the fields is a blue button labeled 'Sign in'.

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



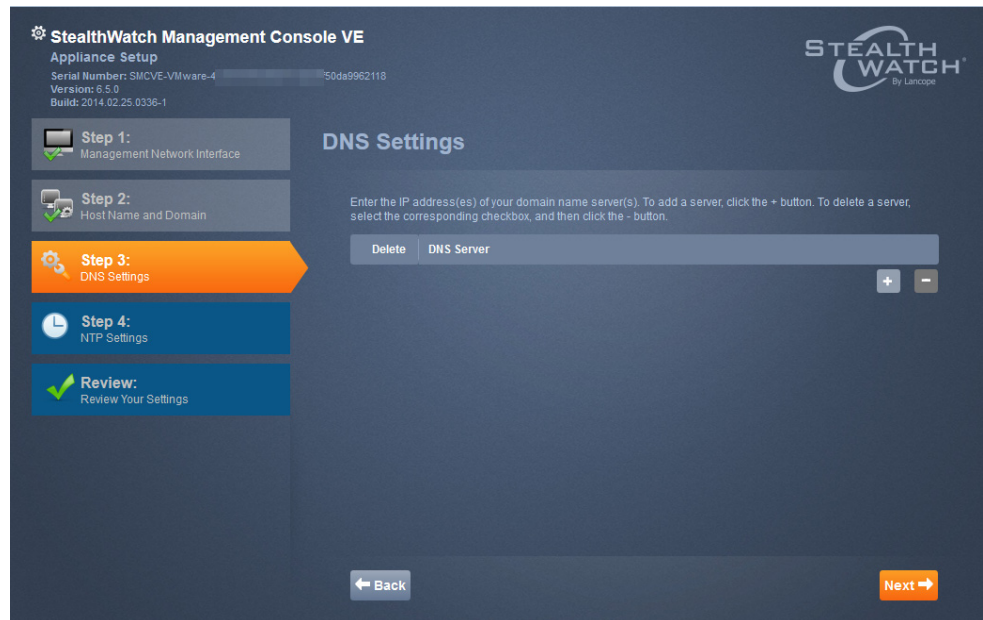
The Management Network Interface page opens.



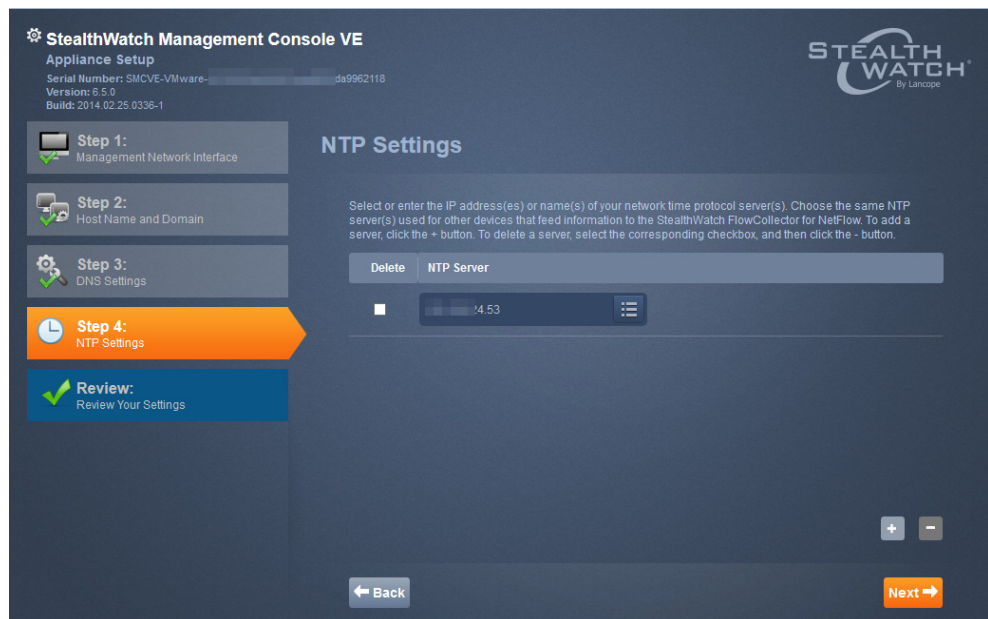
5. Review the settings you previously entered, and then click **Next**. The Host Name and Domain page opens:



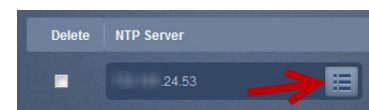
- In the appropriate fields, type the host name and the network domain name, and then click **Next**. The DNS Settings page opens.



- Click the + button, and then type the IP address of the DNS server. Click **Next**. The NTP Settings page opens.



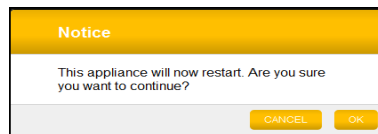
- You can accept the default setting or enter another server by entering the IP address of your NTP server or selecting a name by clicking the list icon and selecting one from the drop-down list.



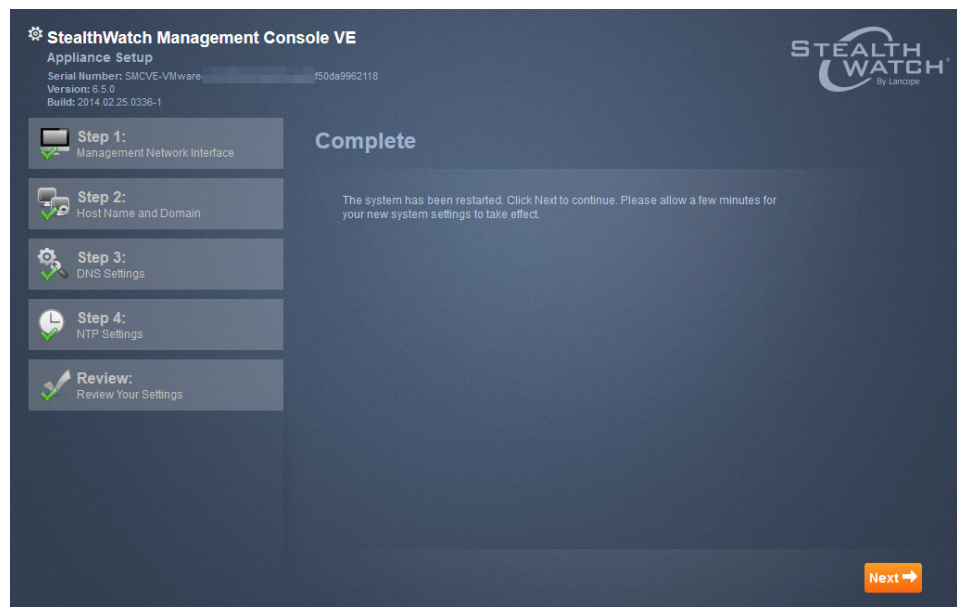
- Click **Next**. The Review page opens.



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



- Click **OK**. The Complete page opens.



12. 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 or the SMC landing page opens.
13. Enter the login credentials if needed, and then click **Login**.
14. 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.
15. 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. Change the Admin Password
4. Configure UDP Director VE Rules
5. Restart the Virtual Appliance

Log in to the Appliance Administration Interface

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



Note:

The supported browsers for StealthWatch are Internet Explorer version 9 and later and Firefox version 3 and later.

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

STEALTH WATCH®
By Lancope
FlowCollector for NetFlow VE
6.6.0

Username:

Password:

Login >>

2. In the **Username** field, type **admin**.

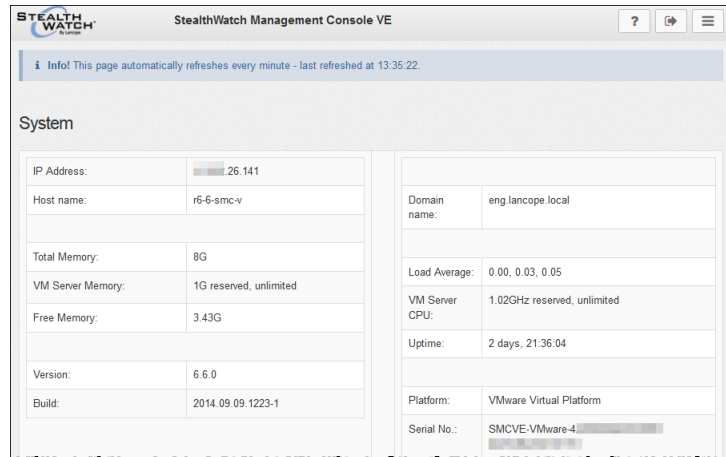
- In the **Password** field, type the default password **lan411cope**.



Important:

To help ensure security, change the admin password after you finish configuring the virtual appliance (**Configuration > Change Password**).

- Click **Login**. The Appliance Admin interface Home page opens.



- Continue with the next section, “Configure the System Time.”

Configure the System Time

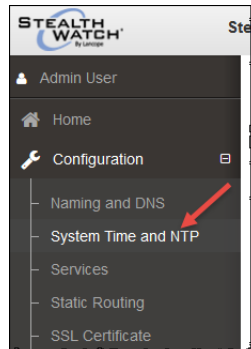
To configure the Network Time Protocol (NTP) and system time (time zone) settings on the virtual appliance, complete the following steps:



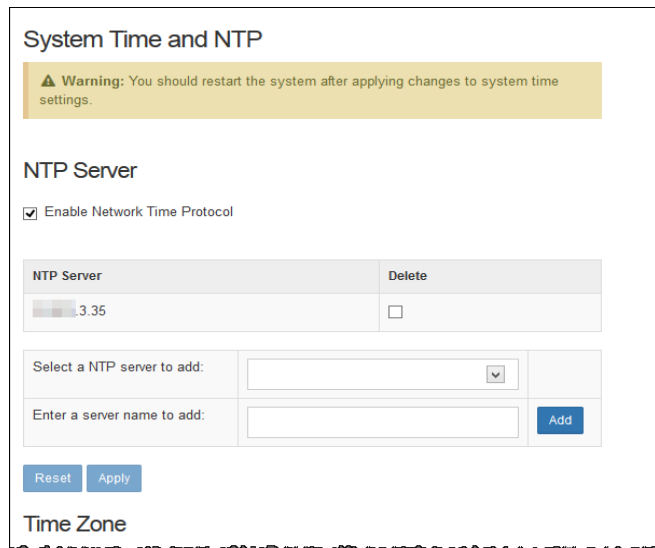
CAUTION:

Use the same NTP server used for the FlowCollectors and other devices that feed information to the SMC.

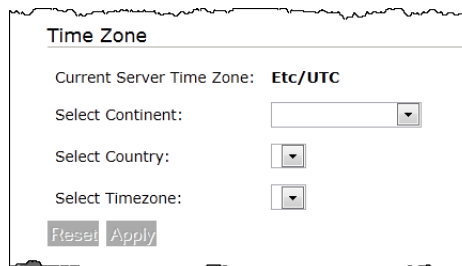
1. On the Appliance Admin interface navigation pane, click the plus sign (+) beside **Configuration** and then click **System Time and NTP**.



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.

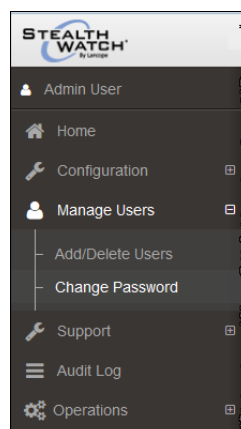
5. Click **OK**.
6. Continue to the next section, “Change the Admin Password.”

Change the Admin Password

To help ensure the security of your network, change the default admin user password. You will restart the system after this procedure.

To change your password, complete the following steps:

1. In the Appliance Admin interface navigation pane, click the plus sign (+) beside **Manage Users** and then click **Change Password**.



The Change Password page opens.

Change Password

i Password Format (Case-Sensitive)

- Must be between 8 and 30 characters.
- Must be different from the previous password by at least 4 characters.

Enter current password:	<input type="password" value="*****"/>
Enter new password:	<input type="text"/>
Confirm new password:	<input type="text"/>
<input type="button" value="Apply"/>	

2. Do the following in the applicable fields:

- ▶ Type the current password, lan411 cope.



Note:

The password must be between 5 and 30 alphanumeric characters in length with no spaces. You also may use the following special characters: \$.~!@#%_=?.,{}()

- ▶ Type the new password.
- ▶ Type the new password again to confirm it.
- ▶ To activate click the **Apply** button.

Change Password

i Password Format (Case-Sensitive)

- Must be between 8 and 30 characters.
- Must be different from the previous password by at least 4 characters.

Enter current password:	<input type="password" value="*****"/>
Enter new password:	<input type="password" value="*****"/>
Confirm new password:	<input type="password" value="*****"/>
<input type="button" value="Apply"/>	

3. Click **Apply** to change the password. The password change confirmation appears.

Password successfully changed.

4. Continue with the next section, ““Configure UDP Director VE Rules.””

Configure UDP Director VE Rules

For the UDP Director VE (also known as FlowReplicator VE), you need to configure the exporter to send flows to be forwarded to the IP address of eth0. The FlowReplicator will then forward these from eth0 while preserving the original IP and MAC address of each exporter for forwarded packets.



Note:

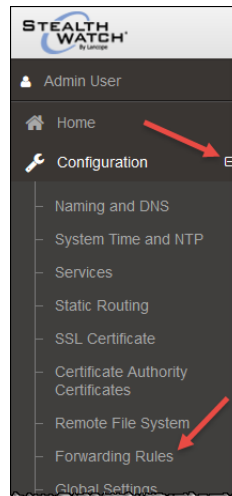
For promiscuous reception, Lancope recommends that you use a span filter for all traffic of interest.

The network must allow traffic on the ports being used from the exporters to the FlowReplicator and then to the receivers (ACLs).



To configure the rules for the FlowReplicator, complete the following steps:

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



The Forwarding Rules page opens.

Forwarding Rules

Rule #	Description	Source IP Address:Port List	Destination IP Address	Destination Port Number	Delete
1.	NFLOW	All:2055	26.103	2055	<input type="checkbox"/>
2.	SFLOW	All:6343	26.105	6343	<input type="checkbox"/>

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 FlowReplicator followed by the port number through which the data will be sent. Use the following syntax:

[IP address]:[Port Number] as in 10.201.1.41:2057

Note:

To receive all traffic from any device from a specific port, type **All:[port number]**. For example, type **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.

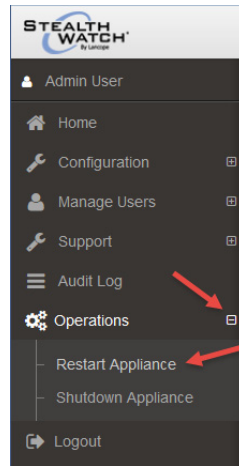
5. In the Destination IP Address field, type the IP address of the device that receives data from the FlowReplicator.
6. In the Destination Port Number field, type the port number for the receiving device.
7. If you have more than one device sending data to the FlowReplicator to be forwarded to another 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 FlowReplicator.
8. When finished, click **Apply**. The FlowReplicator 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, “Restart the Virtual Appliance.”



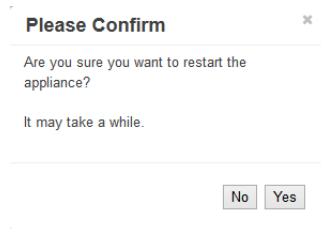
Restart the Virtual Appliance

To restart the virtual appliance, complete the following steps:

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



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.



