StealthWatch® System Hardware Installation Guide

(for StealthWatch System v6.7.0)

Installation Guide: StealthWatch System v6.7.0 Hardware

Document Date: March 19, 2015

Trademarks

CONTENTS

INTRODUCTION

OVERVIEW

This guide explains how to install StealthWatch System products. It describes the StealthWatch System components and how they are placed in the system, including the integration of the FlowSensors. Also, this guide describes the mounting and installation of the StealthWatch System hardware.

This chapter includes the following topics:

- Audience
- How to Use This Guide
- Documentation Icons
- Common Abbreviations
- Other Resources

Audience

This guide is designed for the person responsible for installing StealthWatch system hardware. We assume that you already have some general understanding of installing network equipment (FlowSensor, FlowCollector, UDP Director (also known as FlowReplicator), and the StealthWatch Management Console).

For information on configuring StealthWatch System products, please refer to the *StealthWatch System Hardware Configuration Guide*.

How to Use This Guide

In addition to this introduction, we have divided this guide into the following chapters, as well as an index:

Chapter	Description
2 - Pre-Configuration Considerations	Describes the StealthWatch system components and their placement and the configuration of the firewall for communications
3 - Installation	Describes the mounting and installation of StealthWatch hardware

Documentation Icons

This guide uses the following documentation icons:

Icon	Meaning	Description
📝	Note	Additional information you may find useful
💡	Tip	Helpful information, such as shortcuts or easier ways of performing certain tasks
📣	Important	Information you must observe to prevent significant consequences, such as the malfunction of software
🚧	Caution	Information you must observe to prevent loss of data or damage to hardware
⚠	Warning	Information you must observe to prevent risk of personal injury

Common Abbreviations

The following abbreviations appear in this guide:

Abbreviation	Description
AC	Alternation Current
DMZ	Demilitarized Zone (a perimeter network)
DNS	Domain Name Server/Service
FC	FlowCollector
FS	FlowSensor
FTP	File Transfer Protocol
HTTPS	Hypertext Transfer Protocol (Secure)
Hz	Hertz
IP	Internet Protocol
ISE	Identity Services Engine
Mbps	Megabits per second
ms	Milliseconds
NAT	Network Address Translation
NIC	Network Interface Card
NTP	Network Time Protocol
PCIe	Peripheral Component Interconnect Express
SCP	Secure Copy
SMC	StealthWatch Management Console
SNMP	Simple Network Management Protocol
SPAN	Switch Port Analyzer
SSH	Secure Shell
TAP	Test Access Port
UPS	Uninterruptible Power Supply
URL	Universal Resource Locator
USB	Universal Serial Bus
VLAN	Virtual Local Area Network

Other Resources

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

Related Documents

Please refer to your StealthWatch System Documentation CD for information about StealthWatch appliances and their installation and configuration. Except for the online Help,

Additional information is available in the StealthWatch User Community section of the Lancope Web site (https://community.lancope.com/). If you do not have login access to the User Community, send an Email requesting access to support@lancope.com.

NetFlow Ninjas Blog

Lancope's *NetFlow Ninjas* 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.

StealthWatch Video Library

The StealthWatch online video library (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.
- Call +1 800-838-6574.
- Send an Email to support@lancope.com.
- Submit a case using the Support form on the Lancope Customer Community web site (https://community.lancope.com).

Document Feedback

If you have comments about this document, please contact Lancope at support@lancope.com. We appreciate your feedback.

2

PRE-CONFIGURATION CONSIDERATIONS

OVERVIEW

This chapter examines the considerations you should make before installing and configuring your StealthWatch appliances. It explains where to place StealthWatch system products and how to integrate them into your network.

This chapter includes the following topics.

StealthWatch Components

The StealthWatch system is made up of several hardware components that gather, analyze, and present information about your network to improve network performance and security. This section describes the major StealthWatch components.

StealthWatch Management Console

The StealthWatch Management Console (SMC) is the control center for StealthWatch. It manages, coordinates, configures, and organizes all of the different components of the system. The SMC client software allows you to access the SMC's user-friendly graphical user interface (GUI) from any local computer with access to a Web browser. Through the client GUI, you can easily access real-time security and network information about critical segments throughout your enterprise.

Featuring Java-based platform independence, the SMC enables:

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

FlowCollector

The StealthWatch FlowCollector for NetFlow gathers NetFlow, cFlow, J-Flow, Packeteer 2, NetStream, and IPFIX data to provide cost-effective, behavior-based network protection.

The FlowCollector aggregates high-speed network behavior data from multiple networks or network segments to deliver end-to-end protection and improve performance across geographically dispersed networks.

As the FlowCollector receives data, it identifies known or unknown attacks, internal misuse, or misconfigured network devices, regardless of packet encryption or fragmentation. Once StealthWatch identifies the behavior, the system can take any action you have configured it to take, if any, for that kind of behavior.

FlowSensors

The StealthWatch FlowSensor is a network appliance that operates similarly to a traditional packet capture appliance or IDS in that it plugs into a switch port analyzer (SPAN), mirror port, or Ethernet test access port (TAP). The FlowSensor augments visibility into the following network areas:

- Where NetFlow is not available.
- Where NetFlow is available, but you want deeper visibility into performance metrics and packet data.

By directing the FlowSensor toward any NetFlow v9-capable flow collector you can derive valuable detailed traffic statistics from NetFlow. When combined with the StealthWatch FlowCollector for NetFlow, the FlowSensor 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 FlowSensor 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 FlowCollector for NetFlow.

UDP Director (also known as FlowReplicator)

The StealthWatch UDP Director (also known as FlowReplicator) is a high-speed, high-performance UDP packet replicator. The UDP Director s very helpful in redistributing NetFlow, sFlow, syslog, or Simple Network Management Protocol (SNMP) traps to various collectors. It can receive data from any connectionless UDP application and then retransmit it to multiple destinations, duplicating the data if required.

Note:

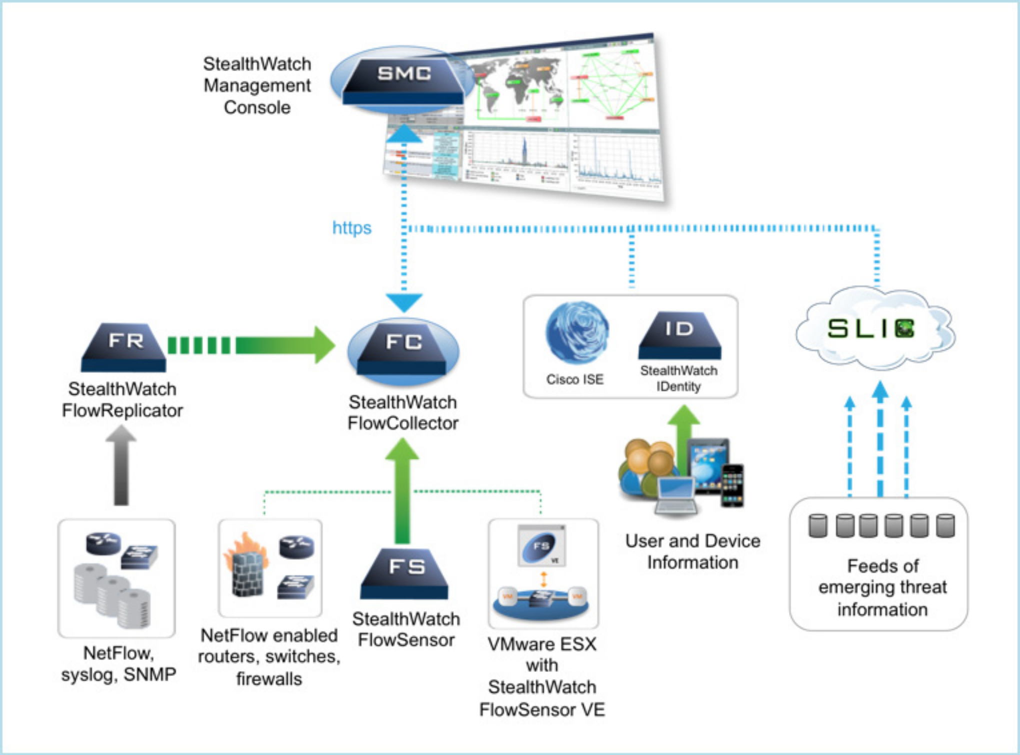
When you use the UDP Director High Availability (HA) configuration (failover), you must connect two UDP Directors with crossover cables. For specific instructions, see “Connecting to the Network” on page 43.

Identity Devices

The StealthWatch system includes identity devices such as the StealthWatch IDentity appliance and the Cisco ISE (Identity Services Engine). These devices map IP addresses to user names by passively pulling user authentication information from user identity databases. The SMC seamlessly manages multiple identity appliances. For information on the installation of StealthWatch IDentity, see its accompanying CD.

Placement Considerations

As shown in the figure below, StealthWatch system products can be strategically deployed to provide optimal coverage of key network segments throughout the network, whether in the internal network, at the perimeter, or in the DMZ.


StealthWatch Management Console
SMC
https
FR
StealthWatch FlowReplicator
FC
StealthWatch FlowCollector
Cisco ISE
ID
StealthWatch IDentity
SLIC
NetFlow, syslog, SNMP
NetFlow enabled routers, switches, firewalls
FS
StealthWatch FlowSensor
FS VE
VM
VMware ESX with StealthWatch FlowSensor VE
User and Device Information
Feeds of emerging threat information

Placing the SMC

As the management device, the StealthWatch Management Console (SMC) should be installed at a location on your network that is accessible to all the devices sending data to it.

If you have a failover pair of SMCs, it is recommended that you install the primary SMC and the secondary SMC in separate physical locations. This strategy will enhance a disaster recovery effort should it become necessary.

Placing the StealthWatch FlowCollector

As collection and monitoring devices, the StealthWatch FlowCollector for NetFlow appliance and the StealthWatch FlowCollector for sFlow appliance should be installed at a location on your network that is accessible to the NetFlow or sFlow devices sending the data to a FlowCollector, as well as any devices you plan to use to access the management interface.

Note:

When you place a FlowCollector outside a firewall, Lancope recommends that you turn off the setting “Accept traffic from any exporter.”

Placing the StealthWatch FlowSensor

As a passive monitoring device, the StealthWatch FlowSensor can sit at multiple points on your network to observe and record IP activity, thereby protecting network integrity and detecting security breaches. The FlowSensor features integrated Web-based management systems that facilitate either centralized or remote management and administration.

The FlowSensor appliance is most effective when placed at critical segments of your corporate network as follows:

- Inside your firewall to monitor traffic and determine if a firewall breach has occurred
- Outside your firewall, monitoring traffic flow to analyze who is threatening your firewall
- At sensitive segments of your network, offering protection from disgruntled employees or hackers with root access
- At remote office locations that constitute vulnerable network extensions
- On your business network for protocol use management (for example, on your transaction services subnet to determine if a hacker is running Telnet or FTP and compromising your customers' financial data)

Placing Other StealthWatch Products

The only requirement for the placement of other StealthWatch products, such as the StealthWatch UDP Director (also known as FlowReplicator), the StealthWatch IDentity appliance, or a VM server containing a StealthWatch FlowSensor Virtual Edition (VE), is that they have an unobstructed communication path to the rest of your StealthWatch products as applicable.

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
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)	3rd 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

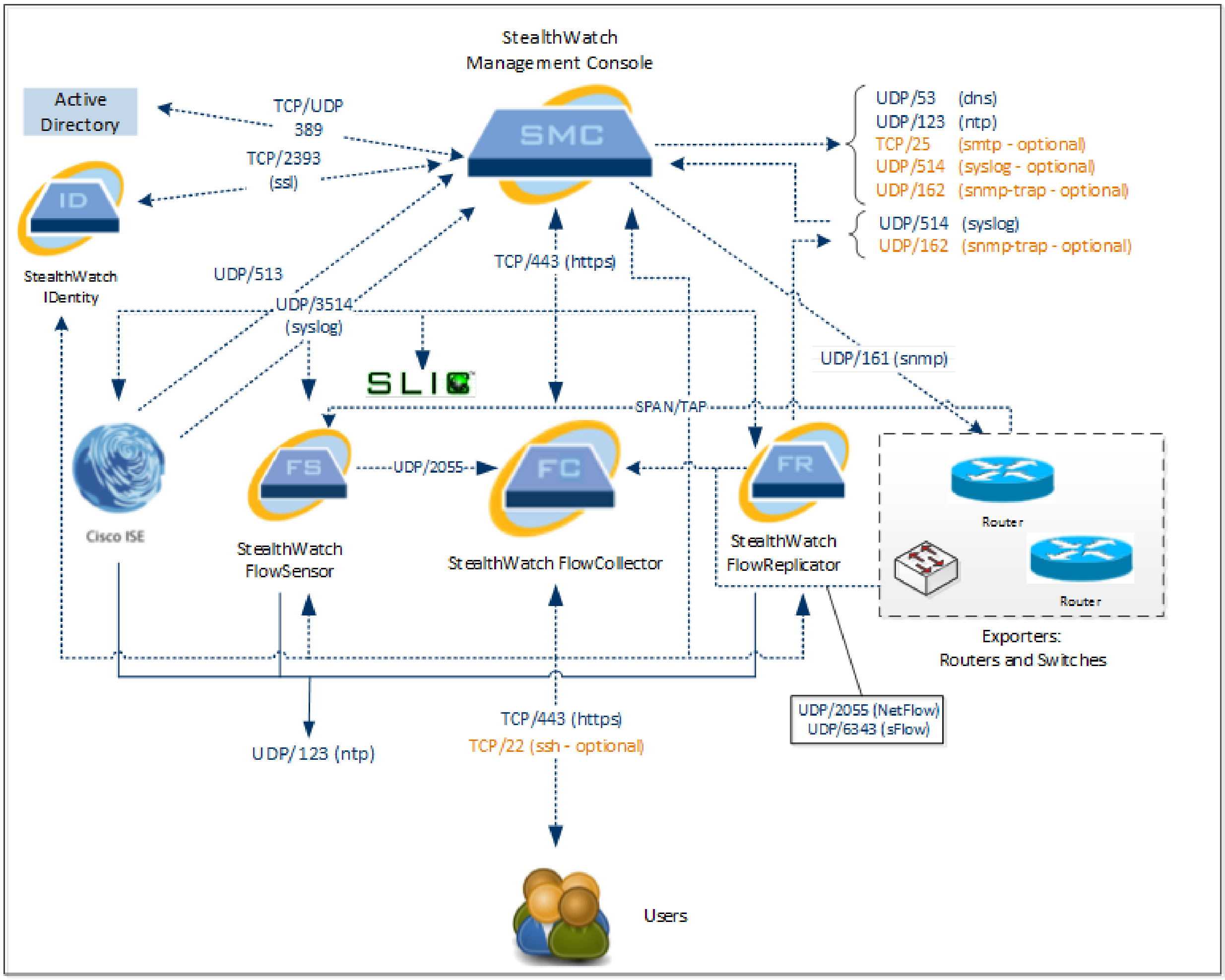
*This is the default port, but any UDP port could be configured on the exporter.

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
SMC	3rd Party event management systems	UDP/162	SNMP-trap
SMC	3rd Party event management systems	UDP/514	SYSLOG

From (Client)	To (Server)	Port	Protocol
- continued -			
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* are ones that may be used according to your own network needs.



INTEGRATING THE FLOWSENSOR INTO YOUR NETWORK

The StealthWatch FlowSensor is versatile enough to integrate with a wide variety of network topologies, technologies, and components. While not all network configurations can be discussed here, the examples may help you determine the best setup for your monitoring needs.

Before you install a FlowSensor, you must make several decisions about your network and how you want to monitor it. Be sure to analyze both your network's topology and your specific monitoring needs. It is recommended that you connect a FlowSensor so that it receives network transmissions to and from the monitored network, and, if desired, receives interior network transmissions as well.

The following sections explain how to integrate a StealthWatch FlowSensor appliance into your network using the following Ethernet network devices:

- TAPs
- SPAN Ports

TAPs

When a Test Access Port (TAP) is placed *in line* with a network connection, it repeats the connection on a separate port or ports. For example, an Ethernet TAP placed in line with an Ethernet cable will repeat each direction of transmission on separate ports. Therefore, use of a TAP is the most reliable way to use the FlowSensor. The type of TAP you use depends on your network.

This section explains the following ways to use TAPs:

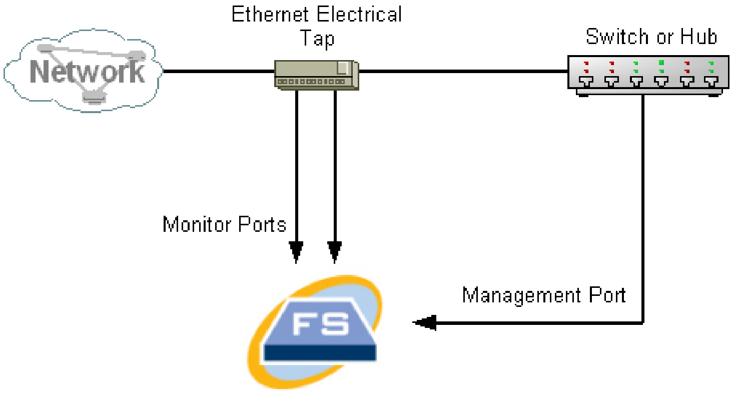
- Using Electrical TAPs
- Using Optical TAPs
- Using TAPs Outside Your Firewall
- Placing the FlowSensor Inside Your Firewall

Note:

In a network using TAPs, the FlowSensor can capture performance monitoring data only if it is connected to an aggregating TAP that is capturing both inbound and outbound traffic. If the FlowSensor is connected to a unidirectional TAP that is capturing only one direction of traffic on each port, then the FlowSensor will not capture performance monitoring data.

Using Electrical TAPs

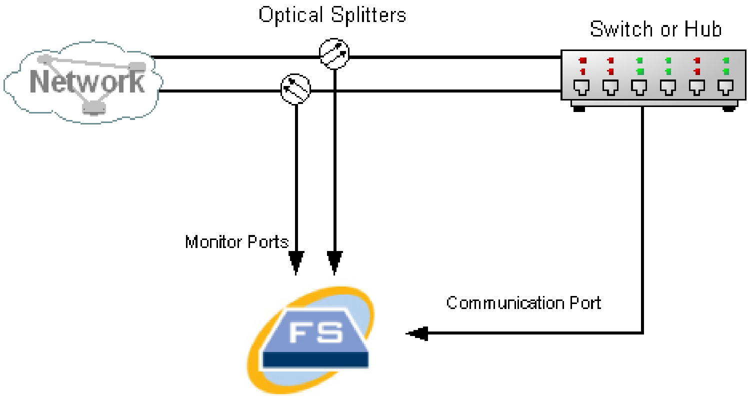
The following illustration shows the StealthWatch FlowSensor connected to an Ethernet electrical TAP. To achieve this configuration, connect the two TAP ports to the FlowSensor Monitor Ports 1 and 2, as shown.



Using Optical TAPs

Two splitters are required for fiber-optic–based systems. You can place a fiber-optic cable splitter in line with each direction of transmission and use it to repeat the optical signal for one direction of transmission.

The following illustration shows the FlowSensor connected to a fiber-optic–based network. To achieve this configuration, connect the outputs of the optical splitters to the FlowSensor Monitor Ports 1 and 2, as shown.



Note:

If the connection between the monitored networks is an optical connection, then the StealthWatch FlowSensor appliance is connected to two optical splitters. The management port is connected to either the switch of the monitored network or to another switch or hub.

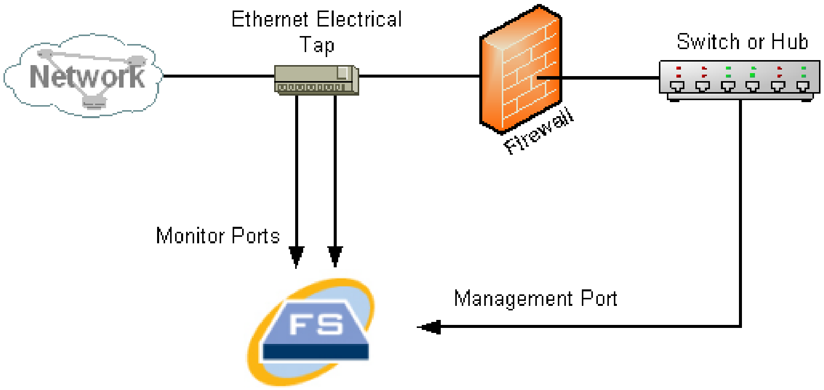
Using TAPs Outside Your Firewall

To have the FlowSensor monitor traffic between your firewall and other networks, connect the StealthWatch management port to a switch or port outside of the firewall.

WARNING:

Lancope strongly recommends that you use a TAP for this connection so that failure of the device does not bring down your entire network.

The following illustration shows an example of this configuration using an Ethernet electrical TAP. The management port must be connected to the switch or hub of the monitored network. This setup is similar to the setup that monitors traffic to and from your network.

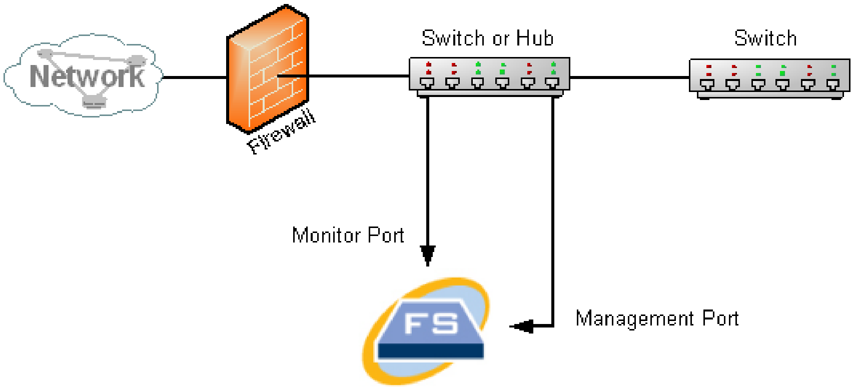


Note:

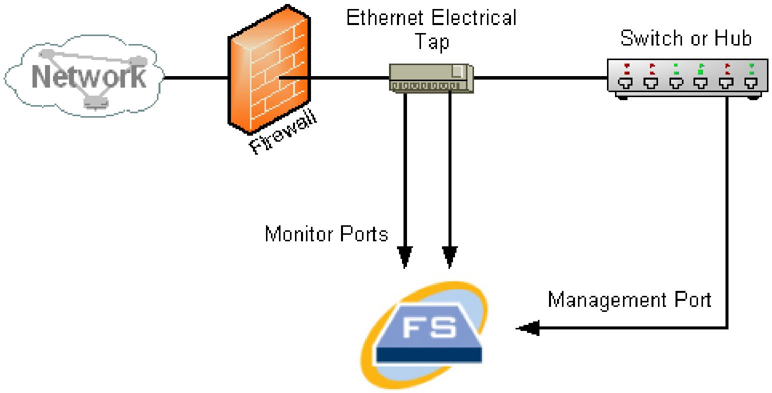
If your firewall is performing network address translation (NAT), you can observe only the addresses that are on the firewall.

Placing the FlowSensor Inside Your Firewall

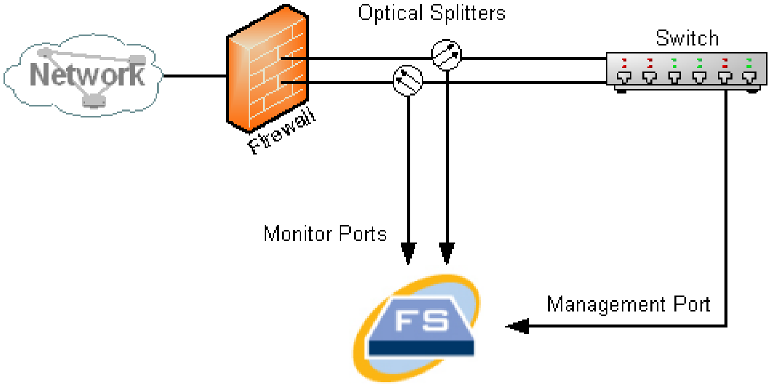
To monitor traffic between internal networks and a firewall, the FlowSensor must be able to access all traffic between the firewall and the internal networks. You can accomplish this by configuring a mirror port that mirrors the connection to the firewall on the main switch. Make sure that the FlowSensor Monitor Port 1 is connected to the mirror port, as shown in the following illustration:



To monitor traffic inside your firewall by using a TAP, insert the TAP or optical splitter between your firewall and the main switch or hub. A TAP configuration is shown below.



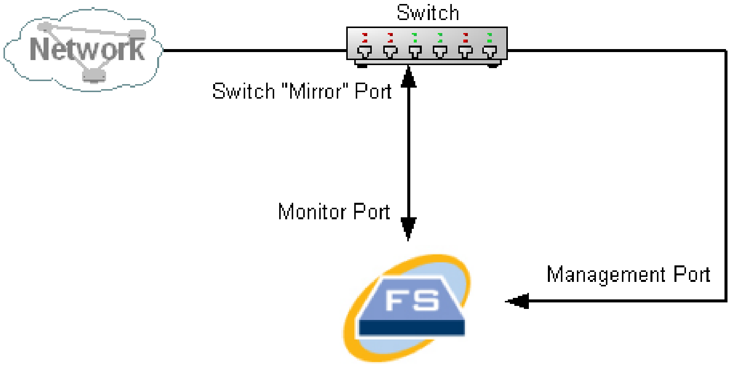
An optical splitter configuration is shown below.



SPAN Ports

You can also connect the FlowSensor to a switch. However, because a switch does not repeat all traffic on each port, the FlowSensor will not perform properly unless the switch can repeat packets transmitted to and from one or more switch ports. This type of switch port is sometimes called a mirror port or Switch Port Analyzer (SPAN).

The following illustration shows how you can achieve this configuration by connecting your network to the StealthWatch FlowSensor through the management port.



In this configuration, you must configure a switch port (also called a mirror port), to repeat all traffic to and from the host of interest to the mirror port. The FlowSensor Monitor Port 1 must be connected to this mirror port. This allows the FlowSensor to monitor traffic to and from the network of interest and to other networks. In this instance, a network may be made up of some or all of the hosts connected to the switch.

A common way of configuring networks on a switch is to zone them into virtual local area networks (VLANs), which are logical rather that physical connections of hosts. If the mirror port is configured to mirror all ports on a VLAN or switch, the FlowSensor can monitor all traffic to, from, and within the network of interest, as well as other networks.

Note:

In all cases, Lancope recommends that you consult your switch manufacturer's documentation to determine how to configure the switch mirror port and what traffic will be repeated to the mirror port.

3

INSTALLATION

OVERVIEW

This chapter includes the procedures for installing the StealthWatch hardware into your environment.

This chapter includes the following topics:

- Mounting the Appliance
- Changing the Default User Passwords
- Connecting the Appliance to the Network

Mounting the Appliance

You can mount StealthWatch products directly in a standard 19" rack or cabinet. You can also install them in any other suitable cabinet or on a flat surface.

Note:

When mounting an appliance in a rack or cabinet, follow the instructions included in the rail mounting kits.

When determining where to place an appliance, make sure that clearance to the front and rear panels is as follows:

- The front-panel indicators can be read easily.
- Access to ports on rear panel is sufficient for unrestricted cabling.
- The rear-panel power inlet is within reach of a conditioned AC power source.
- Airflow around the appliance and through the vents is unrestricted.

Hardware Included with the Appliance

The following hardware is included with StealthWatch System products:

- AC power cord
- Access keys (for front face plate)
- Rail kit for rack mounting, or mounting ears for smaller appliances
- For the FlowCollector 5000, a 10G SFP cable

Additional Required Hardware

You must provide the following additional required hardware:

- Mounting screws for a standard 19" rack
- Uninterruptible power supply (UPS) for each StealthWatch System product you are installing.
- Ethernet cables as shown in the following table, based on the product you are installing and the configuration you ordered. You can use the **Total** columns as a checklist to help you plan for the quantity you need.

Product	Management Port	Monitoring Port(s)	Total Copper	Total Fiber-Optic
FC 1000	1 Copper	1 Copper		

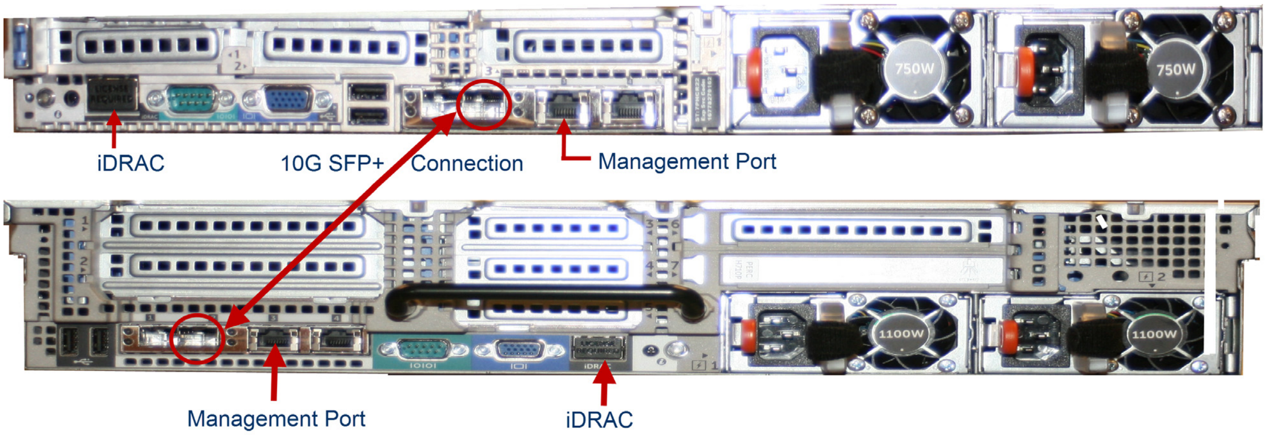
Product	Management Port	Monitoring Port(s)	Total Copper	Total Fiber-Optic
FC 2000	1 Copper	Up to 3 Copper		
FC 4000	1 Copper	Up to 3 Copper		
FC 5000 en	1 Copper	---		
FC 5000 db	1 Copper	---		
FS 250	1 Copper	Up to 2 Copper		
FS 1000	1 Copper	Up to 3 Copper		
FS 2000	1 Copper	Up to 5 Copper **OR** Up to 3 Copper and Up to 2 Fiber-Optic		
FS 3000	1 Copper	Up to 2 Fiber optic		
FR 2000	1 Copper	Up to 3 Copper		
SMC 500	1 Copper	Not Used		
SMC 1000	1 Copper	Not Used		
SMC 2000	1 Copper	Not Used		
Total Ethernet Cables Needed				

- To configure locally (optional), use one of the following methods:
  - Laptop with a video cable and a USB cable (for the keyboard)
  - Video monitor with a video cable and keyboard with a USB cable

FlowCollector 5000

Because the FlowCollector 5000 for NetFlow platform consists of two connected servers the installation differs from other appliances. They are directly connected by a 10G SFP cable so that they function as a single appliance.

The image below shows the connection between the servers. The FlowCollector 5000 engine is above and the database is below.



Note:

The iDRAC Enterprise ports can be used, but Lancope does not support it..

Use the supplied 10G SFP cable to connect these units at the port labeled *eth2*. Place these servers adjacent, vertically, to each other in the rack in order for the 10G SFP cable to reach.

Each server uses a 1G copper Ethernet port to be used as a Management Port. Each server also has a dedicated iDRAC Enterprise port.

Two onboard ports that are not used. These should have a port cover installed to discourage their use.

Changing the Default User Passwords

This section describes how to connect to the appliance and then change the default user passwords.

Connecting to the Appliance

You can connect to the appliance in one of two ways:

- with a keyboard and monitor
- with a laptop (and a terminal emulator)

Note:

For new products, SSH is disabled. You must log into the appliance Administration Web interface to enable it.

Connecting with a Keyboard and a Monitor

To configure the IP address locally, complete the following steps:

1. Plug in the power cable to the appliance.
2. Push the Power button to turn on the appliance and wait for it to finish booting up completely. Do not interrupt the boot up process.

Note:

The power supply fans turn on for some models while the system is not powered on. Check that the LED on the front panel is on.

Be sure to connect the appliance to an uninterruptible power supply (UPS). The power supply requires power or else the system displays an error.

3. Connect the keyboard:
   - If you have a standard keyboard, connect it to the standard keyboard connector.
   - If you have a USB keyboard, connect it to a USB connector.
4. Connect the video cable to the video connector. The login prompt appears.
5. Continue with the section, "Changing the Default IP Addresses" on page 29.

Connecting with a Laptop

You can also connect to the appliance with a laptop, which must have a terminal emulator.

To connect to an appliance with a laptop, complete these steps:

1. Connect your laptop to the appliance using one of the following methods:
   - Connect an RS232 cable from the serial port connector (DB9) on your laptop to the Console Port on the appliance.
   - Connect a crossover cable from the Ethernet port on your laptop to the Management port on the appliance.
2. Boot up your laptop.
3. Connect power to the appliance. Press the Power button to turn on the appliance.

Note:

The power supply fans turn on for some models while the system is not powered on. Check that the LED on the front panel is on.

Be sure to connect the appliance to an uninterruptible power supply (UPS). The power supply requires power or else the system displays an error.

4. On the laptop, make a connection into the appliance.

Note:

You can use any available terminal emulator to communicate with the appliance.

5. Apply the following the settings:
   - BPS: 9600
   - Data bits: 8
   - Stop bit: 1
   - Parity: None
   - Flow Control: None

   The login screen and login prompt are displayed.

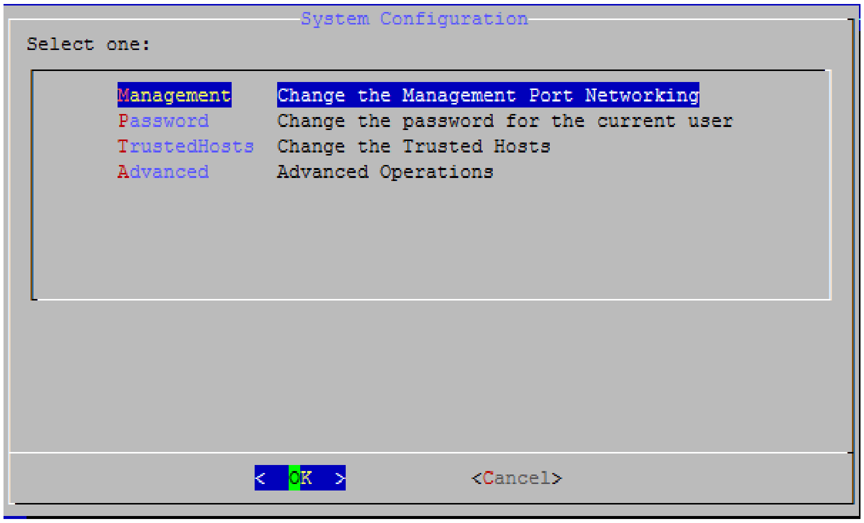
6. Continue with the next section, “Changing the Default IP Addresses.”

Changing the Default IP Addresses

Once you have connected to the appliance, you need to configure the IP addresses. The appliances already have default IP addresses, but you should configure them to suit your network.

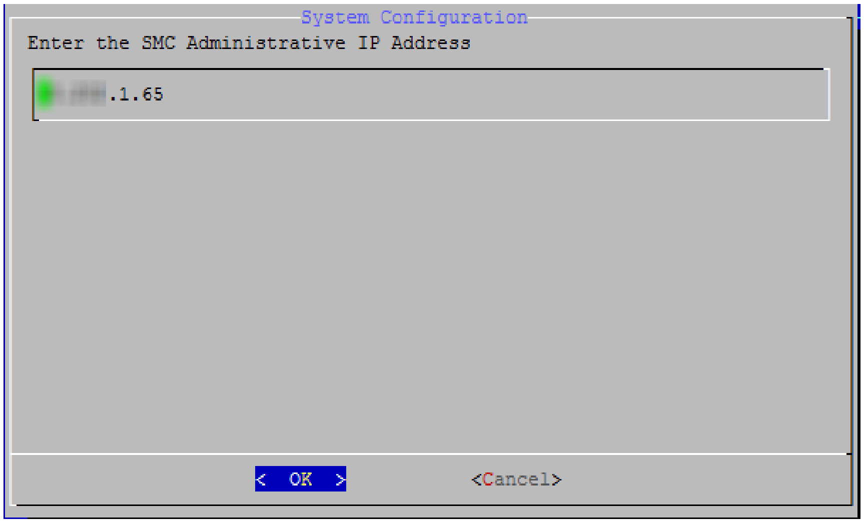
1. Log in to the System Configuration program by doing the following:
   - Type **sysadmin**, and then press **Enter**.
   - When the password prompt appears, type **lan1cope**, and then press **Enter**.
   - At the next prompt, type **SystemConfig**, and then press **Enter**.

   The System Configuration menu opens.



```
System Configuration
Select one:

        Management     Change the Management Port Networking
        Password       Change the password for the current user
        TrustedHosts   Change the Trusted Hosts
        Advanced       Advanced Operations

              <  OK  >              <Cancel>
```

2. Select **Management**, and then press **Enter**. The IP Address page opens.

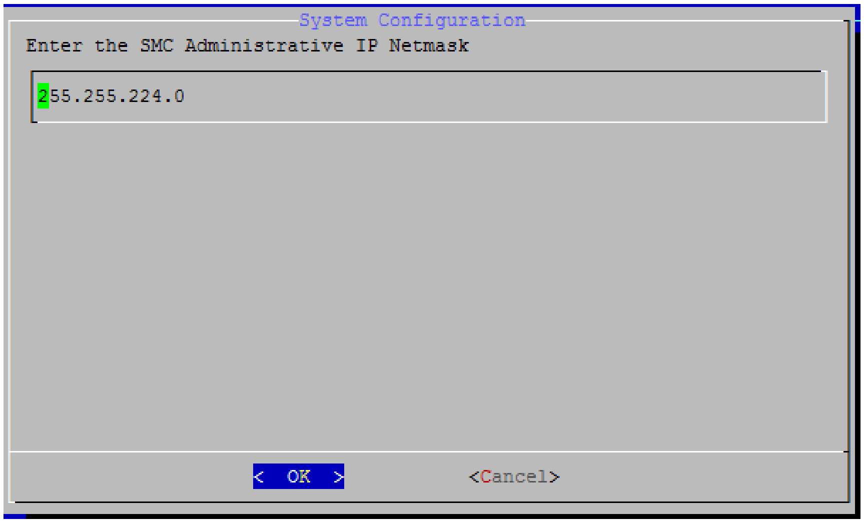


```
System Configuration
Enter the SMC Administrative IP Address

[redacted].1.65

              <  OK  >              <Cancel>
```

3. Do the following:

- Type a new IP address based on your environment.
- Select **OK**, and then press **Enter** to continue.

The IP netmask page opens with the default value.

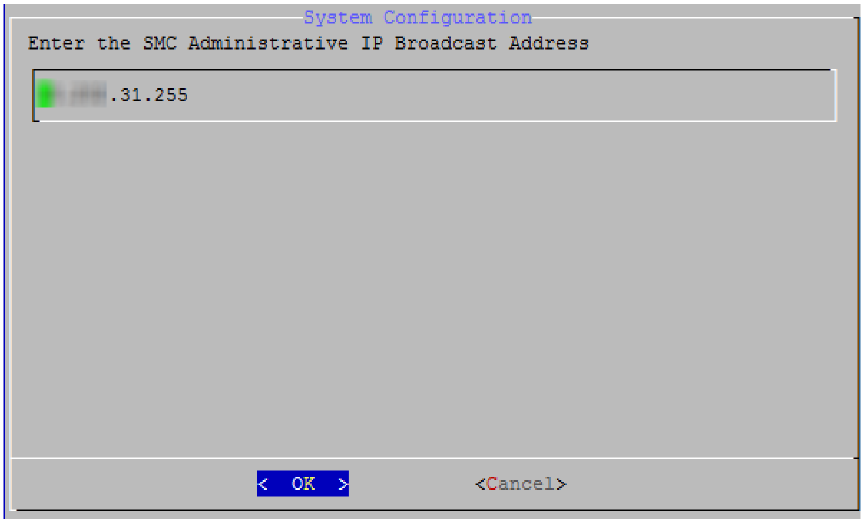


```
System Configuration
Enter the SMC Administrative IP Netmask

255.255.224.0
```

4. Do the following:

- Accept the default value or enter a new IP Netmask address based on your environment.
- Select **OK,** and then press **Enter** to continue.

The Broadcast Address page opens.

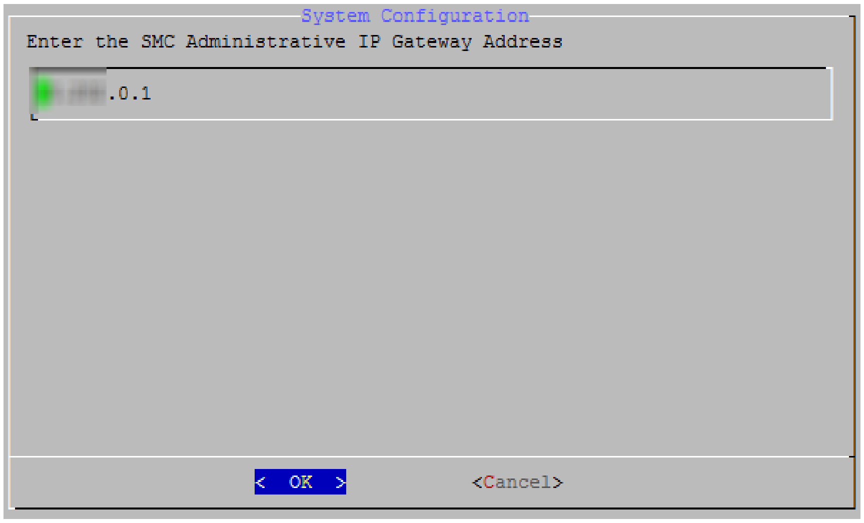


```
System Configuration
Enter the SMC Administrative IP Broadcast Address

[redacted].31.255
```

5. Do the following:

- Accept the default value or enter a new one based on your environment.
- Select **OK**, and then press **Enter** to continue.

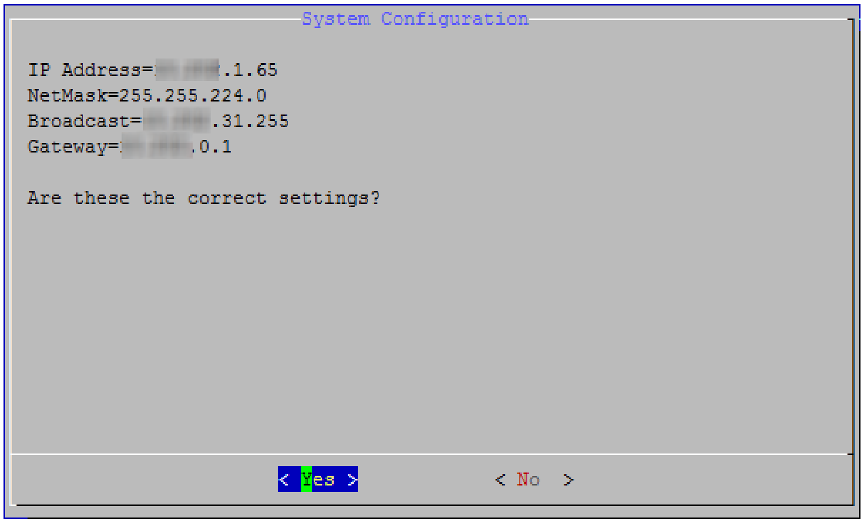
The Gateway Address page opens with the default gateway server IP address.



```
Enter the SMC Administrative IP Gateway Address

[redacted].0.1
```

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

The confirmation page opens.



```
IP Address=[redacted].1.65
NetMask=255.255.224.0
Broadcast=[redacted].31.255
Gateway=[redacted].0.1

Are these the correct settings?
```

7. Review the information. Are the settings correct?
   - If yes, select **Yes,** and then press **Enter** to continue. The system restarts and implements the changes. On completion, the Login page opens.
   - If no, select **No** to make corrections. The IP Address page opens so that you can enter your changes. After the changes are made and you accept the settings, the Restart page opens. Press **Enter** to implement your changes.

8. Continue with the next section, “Connecting the Appliance to the Network.”

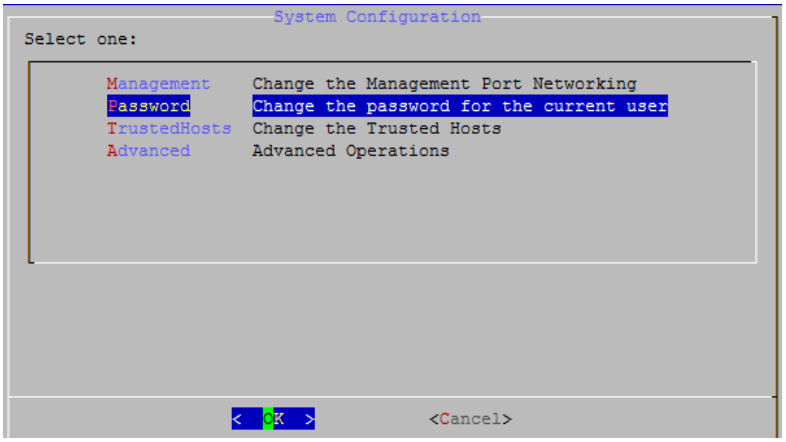
Change the sysadmin User Password

To ensure that your network is secure, you should change the default sysadmin password for appliances.

Note:
Be sure that you have logged in as **sysadmin** to begin this procedure.

To change the sysadmin password, complete the following steps:

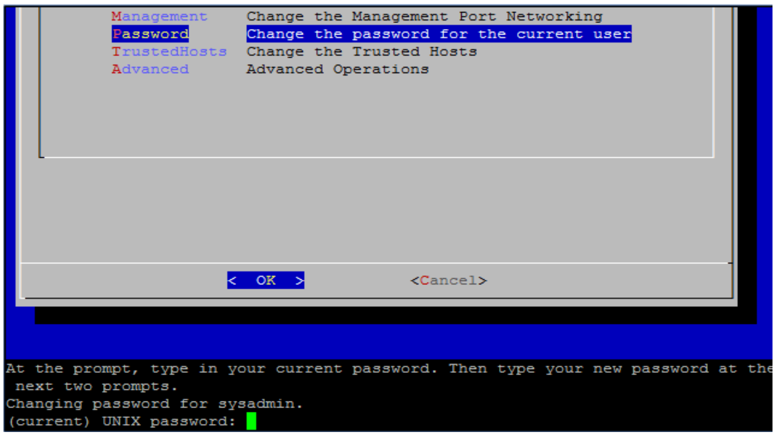
1. On the System Configuration menu, select **Password** and press **Enter**.



```
                        System Configuration
 Select one:

        Management     Change the Management Port Networking
        Password       Change the password for the current user
        TrustedHosts   Change the Trusted Hosts
        Advanced       Advanced Operations



                  <  OK  >             <Cancel>
```

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.

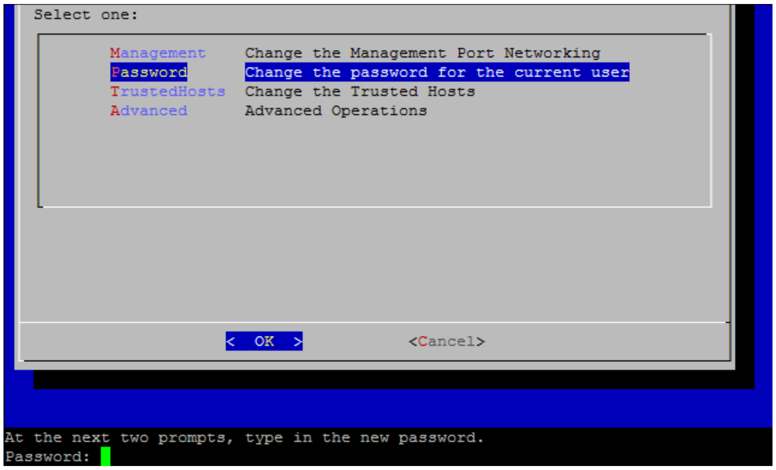
A prompt for the current password appears below the menu.


Management Change the Management Port Networking
Password Change the password for the current user
TrustedHosts Change the Trusted Hosts
Advanced Advanced Operations
< OK >
<Cancel>

```
At the prompt, type in your current password. Then type your new password at the
 next two prompts.
Changing password for sysadmin.
(current) UNIX password:
```

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

   The prompt for a new password appears.


Select one:
Management Change the Management Port Networking
Password Change the password for the current user
TrustedHosts Change the Trusted Hosts
Advanced Advanced Operations
< OK >
<Cancel>

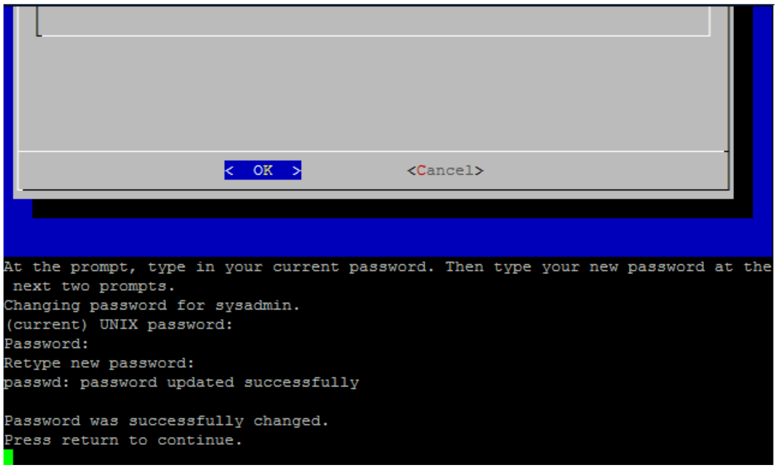
```
At the next two prompts, type in the new password.
Password:
```

3. 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: $.~!@#%_=?:,{}()

4. Type the password again, and then press **Enter**.



```
At the prompt, type in your current password. Then type your new password at the
 next two prompts.
Changing password for sysadmin.
(current) UNIX password:
Password:
Retype new password:
passwd: password updated successfully

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

5. When your password is accepted, press **Enter** again to return to the System Configuration menu.

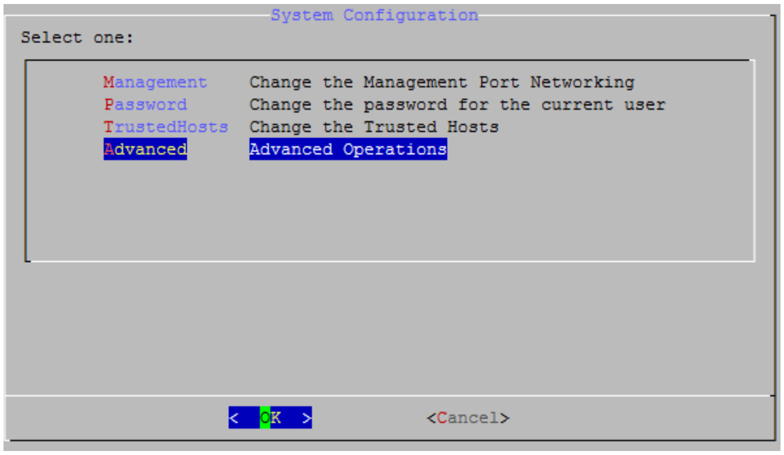
6. Continue with the next section, "Change the root User Password."

Change the root User Password

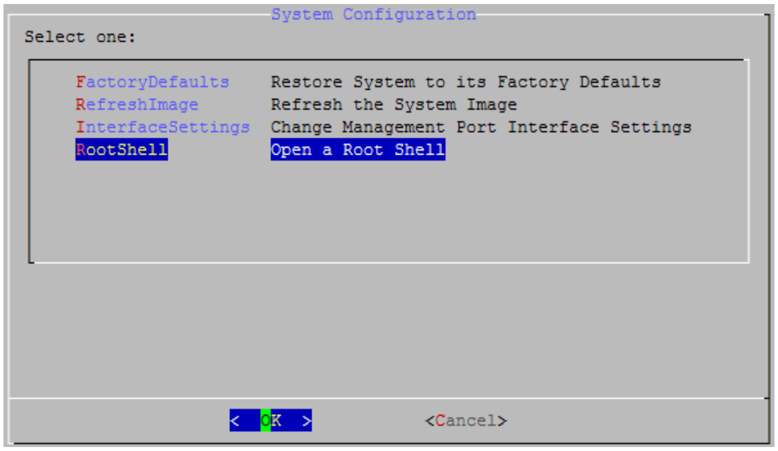
After you change the default sysadmin user password, you need to change the default root user password to protect the security of your network further.

1. To change the root user password, complete the following steps:

   Now in following steps you can change the password for the root login. First you need to go to the root shell.


System Configuration
Select one:
Management Change the Management Port Networking
Password Change the password for the current user
TrustedHosts Change the Trusted Hosts
Advanced Advanced Operations
< OK >
<Cancel>

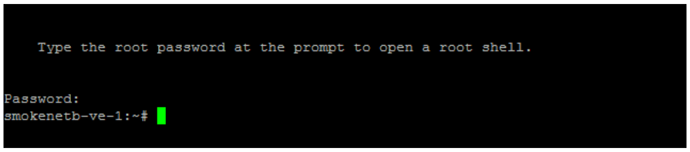
2. On the System Configuration menu, select **Advanced**, and then press **Enter**. The Advanced menu appears.



```
                        System Configuration
 Select one:

    FactoryDefaults     Restore System to its Factory Defaults
    RefreshImage        Refresh the System Image
    InterfaceSettings   Change Management Port Interface Settings
    RootShell           Open a Root Shell

                 <  OK  >          <Cancel>
```

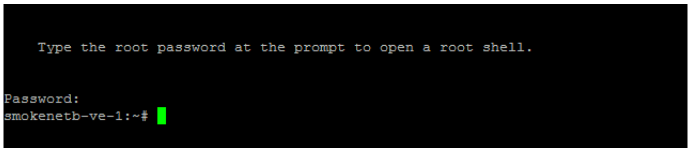
3. Select **RootShell**, and then press **Enter**.

   A prompt for the root password appears.



```
   Type the root password at the prompt to open a root shell.

Password:
smokenetb-ve-1:~#
```

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

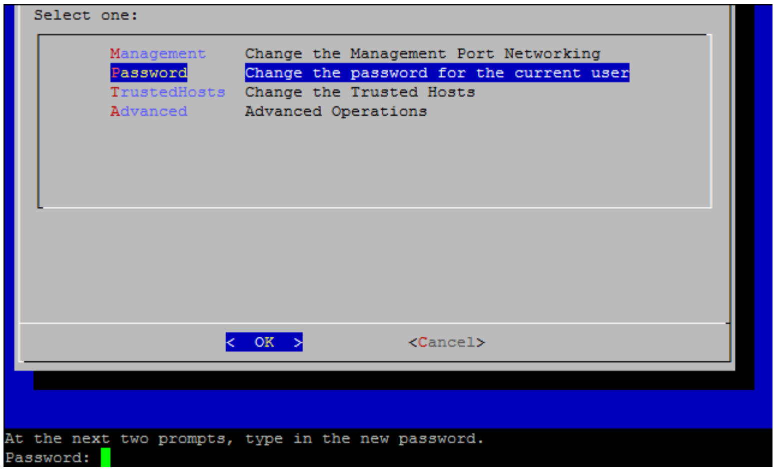


```
   Type the root password at the prompt to open a root shell.

Password:
smokenetb-ve-1:~#
```

5. Type **SystemConfig**, and then press **Enter**.

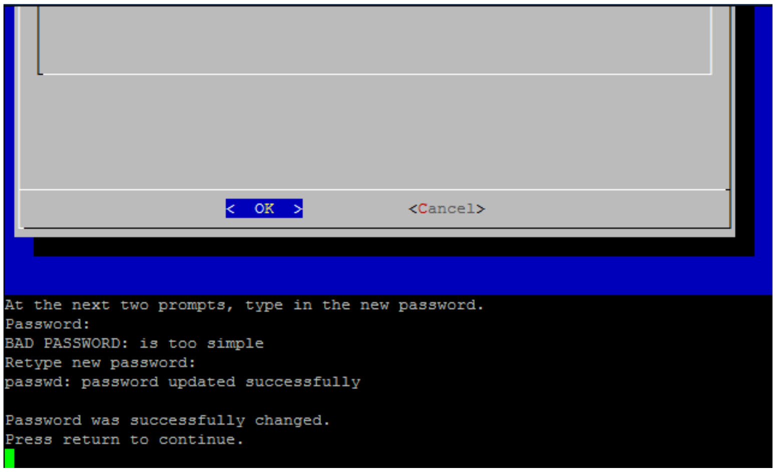
   This returns you to the System Configuration menu so that you can change the root password.

6. Select **Password**, and then press **Enter**. The password prompt appears below the menu.


Select one:
Management Change the Management Port Networking
Password Change the password for the current user
TrustedHosts Change the Trusted Hosts
Advanced Advanced Operations
< OK >
<Cancel>

```
At the next two prompts, type in the new password.
Password:
```

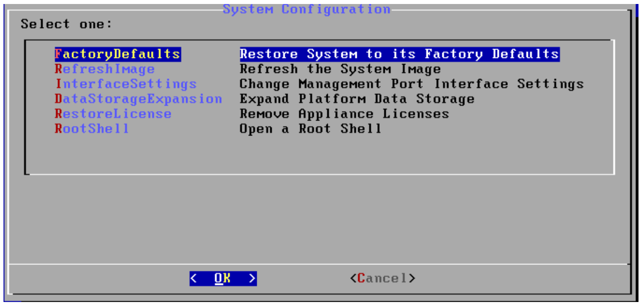
7. Type the new root password, and then press **Enter**. A second prompt appears.



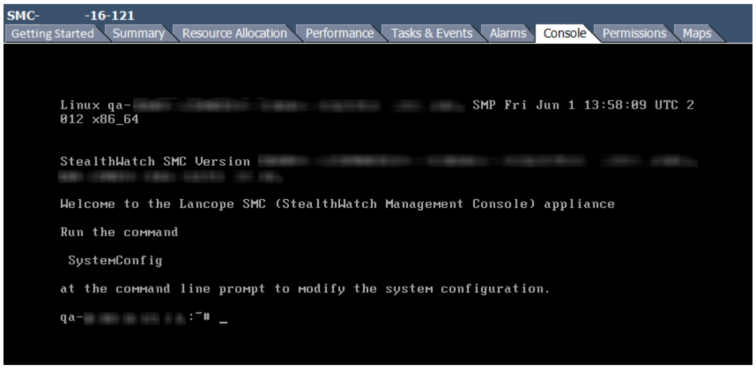
```
At the next two prompts, type in the new password.
Password:
BAD PASSWORD: is too simple
Retype new password:
passwd: password updated successfully

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

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

9. When your password change is successful, press **Enter**. You have now changed both of your default sysadmin and root passwords.This returns you to the System Configuration Console menu.


System Configuration
Select one:
FactoryDefaults Restore System to its Factory Defaults
RefreshImage Refresh the System Image
InterfaceSettings Change Management Port Interface Settings
DataStorageExpansion Expand Platform Data Storage
RestoreLicense Remove Appliance Licenses
RootShell Open a Root Shell
< OK >
<Cancel>

10. Select **Cancel** and press **Enter**. The System Configuration Console closes and the root shell prompt appears.



```
Linux qa-[redacted] SMP Fri Jun 1 13:58:09 UTC 2
012 x86_64

StealthWatch SMC Version [redacted]

Welcome to the Lancope SMC (StealthWatch Management Console) appliance

Run the command

 SystemConfig

at the command line prompt to modify the system configuration.

qa-[redacted]:~# _
```

11. Type **exit** and press **Enter**. The login prompt appears

12. Press **Ctrl+Alt** to exit the Console environment.

13. Continue with the next section, “Connecting the Appliance to the Network.”

Connecting the Appliance to the Network

The procedure to connect each appliance to the network is the same. The only difference for connection is type of appliance you have.

To connect your appliance to the network, complete the following steps:

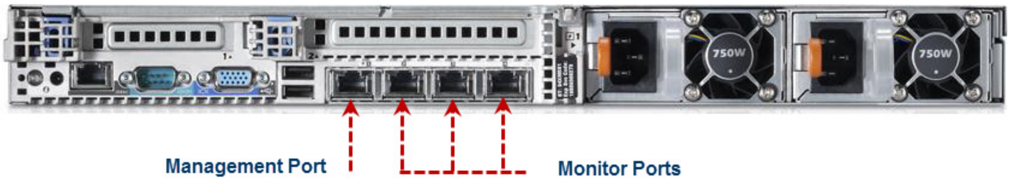
1. Select your appliance from the types of servers shown below.
2. Follow the procedure for connecting the appliance to the network in the section, "Connecting to the Network" on page 43.

Types of Servers

This section illustrates the types of StealthWatch appliances used in a network.

SMCs 1000 & 2000 and FlowCollectors 1000 & 2000

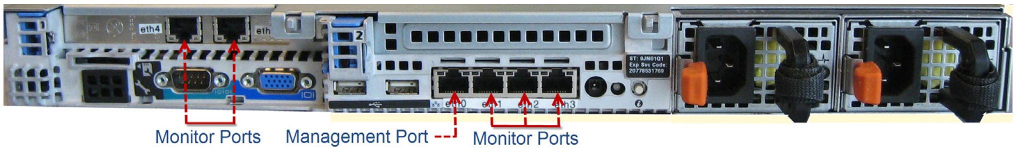
This appliance is used for the SMCs 500/1000, 1000 and 2000, the FlowCollectors 1000 and 2000, and the FlowSensors 2000 and 3000.



Height: 1.68 inches (4.3 cm) **Width:** 18.99 inches (48.24 cm) with rack latches 17.08 (43.4 cm) without rack latches **Depth:** 27.8 inches (70.67 cm) with power supplies and bezel 28.6 inches (72.53 cm) without power supplies and bezel	
Heat Dissipation: 2,891 BTUs per hour maximum **Power:** Redundant, hot swappable: 750W, 50/60 Hz; Auto Ranging (100V to 240V)	

UDP Director 2000, FlowSensors 2000 and 3000

This appliance is the same as the previous one, but it also has two optional fiber optics ports. It is used for the FlowSensor 2000, the FlowSensor 3000, and the UDP Director (also known as FlowReplicator) 2000:

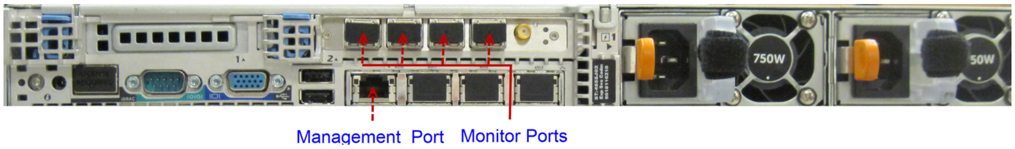


Height: 1.68 inches (4.26 cm)
Width: 18.99 inches (48.24 cm) with rack latches
17.08 (43.4 cm) without rack latches
Depth: 27.8 inches (70.67 cm) with power supplies and bezel
28.6 (72.53 cm) without power supplies and bezel

Heat Dissipation: 2,891 BTUs per hour maximum
Power: 750 W AC, 50/60 Hz; Auto Ranging (100V to 240V)

FlowSensor 4000

The same appliance for the FlowSensor 2000 and FlowSensor 3000 is used for the FlowSensor 4000. However, this FlowSensor supports only 10 GB interfaces and has four monitor ports.

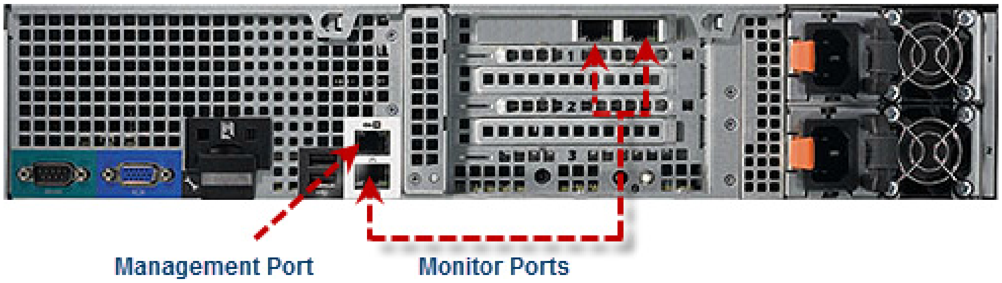


Height: 1.68 inches (4.26 cm)
Width: 18.99 inches (48.24 cm) with rack latches
16.69 (42.4 cm) without rack latches
Depth: 30.39 inches (77.2 cm) with power supplies and bezel
29.02 (73.73 cm) without power supplies and bezel

Heat Dissipation: 2446.5 BTUs per hour maximum
Power: Redundant, hot swappable; 717W

FlowCollector 4000

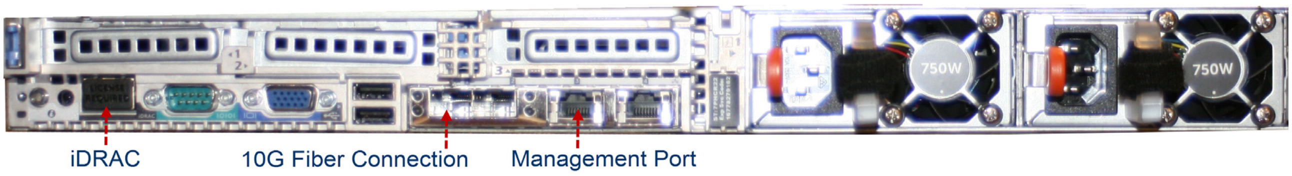
This appliance is used for the FlowCollector 4000



Height: 3.42 inches (8.67 cm) **Width:** 17.53 inches (44.52 cm) **Depth:** 26.17 inches (66.46 cm)	**Heat Dissipation:** 2,559 BTUs per hour **Power:** 2 redundant hot-swappable 750W; Auto Ranging (100V ~ 250V)

FlowCollector 5000 Engine

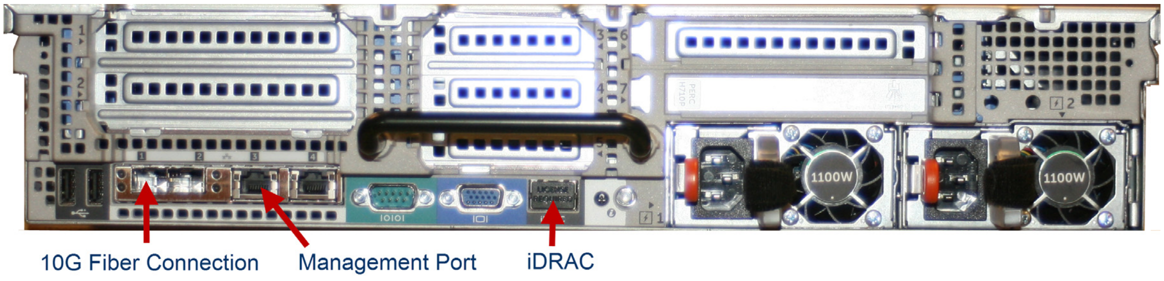
This appliance is used for the FlowCollector 5000, which is paired with the FlowCollector 5000 database.



Height: 1.68 inches (4.26 cm) **Width:** 18.99 inches (48.24 cm) with rack latches 17.08 (43.4 cm) without rack latches **Depth:** 27.8 inches (70.67 cm) with power supplies and bezel 28.6 (72.53 cm) without power supplies and bezel
Heat Dissipation: 2,891 BTUs per hour maximum **Power:** 1100 W AC, 50/60 Hz; Auto Ranging (100V to 240V) (The picture shows 750W power, but the production FlowCollector 5000 uses redundant 1100W power for both the engine and the database

FlowCollector 5000 Database.

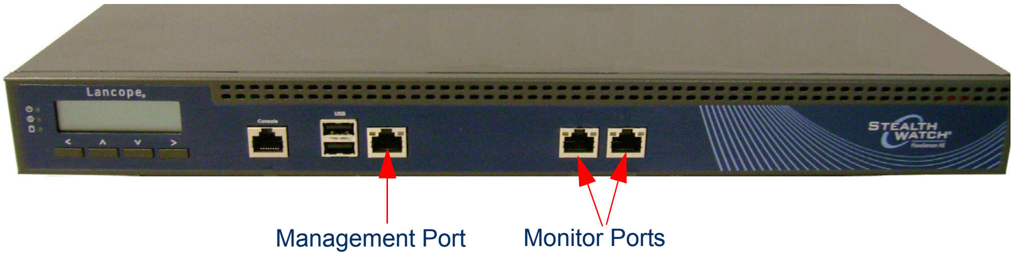
This appliance is used for the FlowCollector 5000 database, which is paired with the FlowCollector 5000 engine.



Height: 3.42 inches (8.67 cm) **Width:** 18.99 inches (48.24 cm) **Depth:** 32.02 inches (81.33 cm)	**Heat Dissipation:** 2,891 BTUs per hour **Power:** 2 redundant hot-swappable 750W; Auto Ranging (100V ~ 240V)

FlowSensor 250

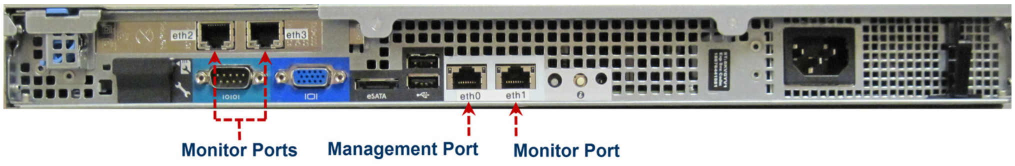
This appliance is used for the FlowSensor 250.



Height: 1.75 inches (4.4 cm) **Width:** 16.93 inches (43 cm) **Depth:** 10.83 inches (27.5 cm)	**Heat Dissipation:** 341 BTUs per hour **Power:** Single: 100W

FlowSensor 1000 and UDP Director (also known as Flow-Replicator) 1000

This appliance is used for the FlowSensor 1000 and the UDP Director 1000.

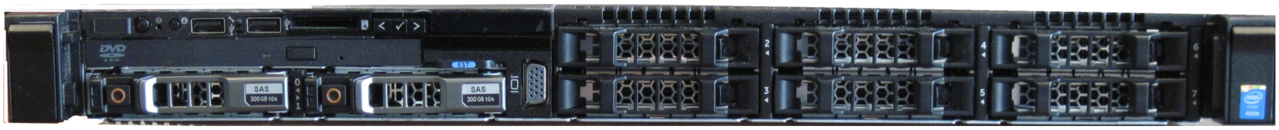


Height: 1.67 inches (4.2 cm) **Width:** 17.09 inches (43.4 cm) **Depth:** 15.5 inches (39.4 cm)	**Heat Dissipation:** 1039 BTUs per hour **Power:** Single: 250W

SMC 1010, FlowCollectors 1010 & 4010, FlowSensors 2010, 3010, 4010 and UDP Director 2010

This appliance is used for the following models:

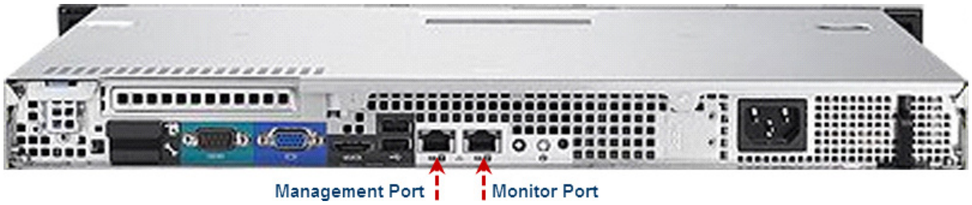
- SMC 1010
- FlowCollector 1010, FlowCollector 4010
- FlowSensor, 2010, FlowSensor 3010, FlowSensor 4010
- UDP Director 2010



Height: 1.68 inches (4.3 cm) **Width:** 17.09 inches (43.4 cm) **Depth:** 29.25 inches (74.3 cm)	**Heat Dissipation:** 2,891 BTUs per hour **Power:** Redundant: 750W

FlowSensor 1010 and UDP Director 1010

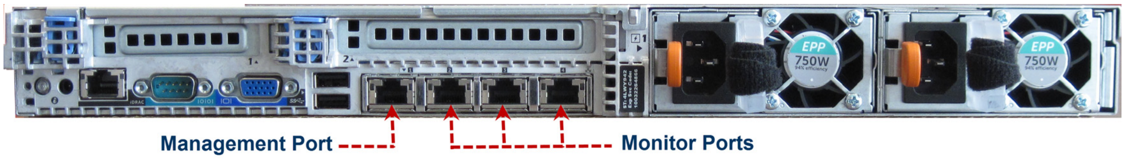
This appliance is used for the FlowSensor 1010 and the UDP Director 1010.



Height: 1.67 inches (4.2 cm) **Width:** 17.09 inches (43.4 cm) **Depth:** 15.5 inches (39.4 cm)	**Heat Dissipation:** 1040 BTUs per hour **Power:** Single: 250W

SMC 2010 and FlowCollector 2010

This appliance is used for the SMC 2010 and the FlowCollector 2010



Height: 1.68 inches (4.3 cm) **Width:** 17.09 inches (43.4 cm) **Depth:** 29.25 inches (74.3 cm)	**Heat Dissipation:** 2,891 BTUs per hour **Power:** Redundant: 750W

Connecting to the Network

To connect the appliance to your network, complete the following steps:

1. Connect an Ethernet cable to the management port, located at the rear of the appliance.
2. Connect at least one monitor port for FlowSensors and UDP Directors (also known as FlowReplicators). Refer to the hardware table on page 24 for the appropriate cable for your appliance.)

Important:

For the UDP Director (also known as FlowReplicator) HA, connect the two UDP Directors by crossover cables. Connect the eth2 port of one UDP Director (also known as FlowReplicator) to the eth2 port of the second UDP Director. Similarly, connect the eth3 port of each UDP Director with a second crossover cable. The cable can be fiber or copper.

Note:

Be sure to note the Ethernet label (eth2, eth3, etc.) for each port. These labels correspond to the network interfaces (eth2, eth3, etc.) that are displayed on, and may be configured from, the Home page of the Appliance Admin interface.

3. Connect the other end of the Ethernet cables to your network's switch.
4. Connect the power cords to the power supply. Some appliances have two power connections: Power Supply 1 and Power Supply 2.
5. Push the Power button to turn on the appliance.

Note:

You may need to remove the front panel to apply power. The power supply fans turn on for some models while the system is not powered on. Check that the LED on the front panel is on.

Be sure to connect the appliance to a UPS. Both power supplies require power or else the system displays an error.

6. To configure the appliance, see the *StealthWatch System Hardware Configuration Guide*.

www.lancope.com