



Cisco Stealthwatch

x210 Series Hardware Installation Guide



Table of Contents

Introduction	4
Overview	4
Audience	4
How to Use This Guide	5
Common Abbreviations	5
Pre-Configuration Considerations	6
Logging in using the CIMC Default Password	6
About Stealthwatch Appliances	6
Stealthwatch Management Console 2210	6
Stealthwatch Flow Collector 4210 and 5210	7
Stealthwatch Flow Sensor 1210, 3210, and 4210	7
Stealthwatch UDP Director 2210	8
Placing Your Appliances	8
Placing the Stealthwatch Management Console	9
Placing the Stealthwatch Flow Collector	9
Placing the Stealthwatch Flow Sensor	9
Placing the Stealthwatch UDP Director	10
Configuring Your Firewall for Communications	10
Communication Ports	12
Integrating the Flow Sensor into Your Network	16
TAPs	16
Using Electrical TAPs	17
Using Optical TAPs	17
Using TAPs Outside Your Firewall	18
Placing the Flow Sensor Inside Your Firewall	19
SPAN Ports	20
Installation Preparation	22

Installation Warnings	22
Installation Guidelines	24
Safety Recommendations	26
Maintain Safety with Electricity	26
Prevent ESD Damage	27
Site Environment	27
Power Supply Considerations	27
Rack Configuration Considerations	28
Installation	29
Mounting Your Appliance	29
Hardware Included with the Appliance	29
Additional Required Hardware	29
Connecting Your Appliance to the Network	30
Connecting to Your Appliance	31
Connecting with a Keyboard and a Monitor	31
Connecting with a Laptop	32
Changing Default Information	33
Changing the Default IP Addresses	33
Changing the Sysadmin User Password	37
Changing the Root User Password	39
Configuring Your Appliance	42

Introduction


Overview

This guide explains how to install Stealthwatch x210 Series hardware appliances. It describes the Stealthwatch components and how they are placed in the system, including the integration of Flow Sensors. This guide also describes the mounting and installation of the Stealthwatch hardware. Hardware in the x210 Series includes:

Appliance	Part Number
Stealthwatch Flow Collector 4210	ST-FC4210-K9
Stealthwatch Flow Collector 5210 Engine	ST-FC5210-E
Stealthwatch Flow Collector 5210 Database	ST-FC5210-D
Stealthwatch Flow Sensor 1210	ST-FS1210-K9
Stealthwatch Flow Sensor 3210	ST-FS3210-K9
Stealthwatch Flow Sensor 4210	ST-FS4210-K9
Stealthwatch Management Console 2210	ST-SMC2210-K9
Stealthwatch UDP Director 2210	ST-UDP2210-K9

Audience

This guide is designed for the person responsible for installing Stealthwatch hardware. We assume that you already have some general understanding of installing network equipment (Flow Sensor, Flow Collector, UDP Director, and the Stealthwatch Management Console).

 For information on configuring Stealthwatch appliances, refer to the applicable [Stealthwatch Installation and Configuration Guide](#) for your software version. The x210 Series is compatible with Stealthwatch 7.x software versions.

How to Use This Guide

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

Chapter	Description
2 - Pre-Configuration Considerations	Stealthwatch components, their placement, and configuring the firewall for communications
3 - Installation Preparation	Safety guidelines, warnings, and recommendations
4 - Installation	Mounting and installing Stealthwatch hardware

Common Abbreviations

The following abbreviations appear in this guide:

Abbreviation	Description
DMZ	Demilitarized Zone (a perimeter network)
HTTPS	Hypertext Transfer Protocol (Secure)
ISE	Identity Services Engine
NIC	Network Interface Card
NTP	Network Time Protocol
PCIe	Peripheral Component Interconnect Express
SNMP	Simple Network Management Protocol
SPAN	Switch Port Analyzer
TAP	Test Access Port
UPS	Uninterruptible Power Supply
VLAN	Virtual Local Area Network

Pre-Configuration Considerations

This section examines the considerations you should make before installing and configuring your Stealthwatch appliances. It explains where to place Stealthwatch appliances and how to integrate them into your network. It includes:

- [Logging in using the CIMC Default Password](#)
- [About Stealthwatch Appliances](#)
- [Placing Your Appliances](#)
- [Communication Ports](#)
- [Integrating the Flow Sensor into Your Network](#)

Logging in using the CIMC Default Password

The Cisco Integrated Management Controller (CIMC) enables access to the server configuration and a virtual server console, as well as monitors for hardware health. Log in to the CIMC as Admin and type **password** in the Password field.

Once you log in, change the default password to protect the security of your network.

About Stealthwatch Appliances

Stealthwatch comprises several hardware appliances that gather, analyze, and present information about your network to improve network performance and security. This section describes each Stealthwatch x210 Series appliance.



For more information, refer to specification sheets for each Stealthwatch x210 Series appliance.

Stealthwatch Management Console 2210

The Stealthwatch Management Console manages, coordinates, configures, and organizes all of the different components of the system. Stealthwatch software allows you to access the console's web UI from any computer with access to a web browser. You can easily access real-time security and network information about critical segments throughout your enterprise. Featuring Java-based platform independence, the Stealthwatch Management Console enables:

- Centralized management, configuration, and reporting for up to 25 Stealthwatch Flow Collectors
- Graphical charts for visualizing traffic

- Drill-down analysis for troubleshooting
- Consolidated and customizable reports
- Trend analysis
- Performance monitoring
- Immediate notification of security breaches

Stealthwatch Flow Collector 4210 and 5210

The Stealthwatch Flow Collector gathers NetFlow, cFlow, J-Flow, Packeteer 2, NetStream, and IPFIX data to provide behavior-based network protection.

The Flow Collector 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 Flow Collector receives data, it identifies known or unknown attacks, internal misuse, and misconfigured network devices, regardless of packet encryption or fragmentation. Once Stealthwatch identifies the behavior, the system can take any action you have configured, if any, for that kind of behavior.

Stealthwatch Flow Sensor 1210, 3210, and 4210

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

Because the Flow Sensor 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 Flow Collector.

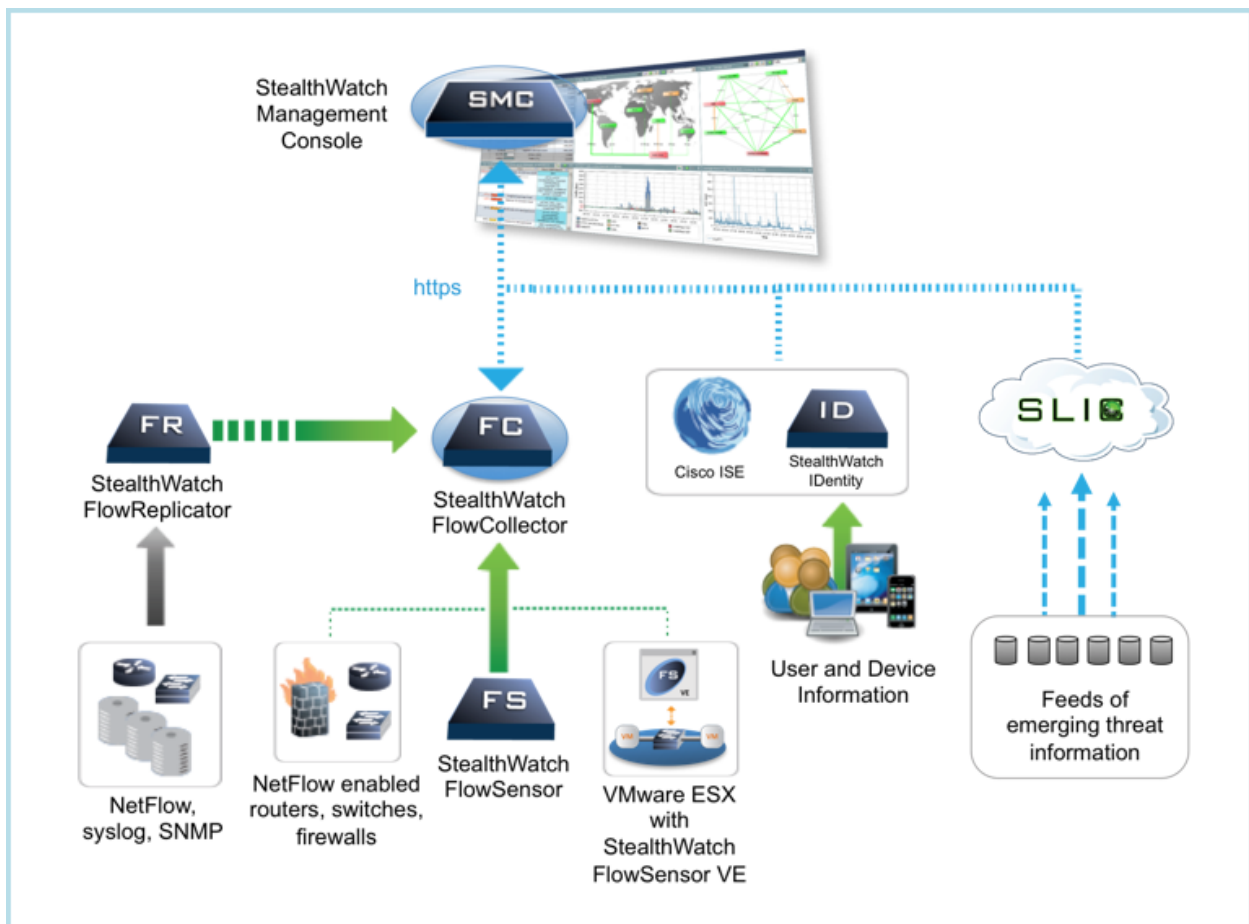
Stealthwatch UDP Director 2210

The Stealthwatch UDP Director is a high-speed, high-performance UDP packet replicator. The UDP Director is 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.

When you use the UDP Director High Availability (HA) configuration (failover), you must connect two UDP Director appliances with crossover cables. For specific instructions, see [Connecting Your Appliance to the Network](#).

Placing Your Appliances

As shown in the figure below, you can strategically deplopy Stealthwatch appliances to provide optimal coverage of key network segments throughout the network, whether in the internal network, at the perimeter, or in the DMZ.



Placing the Stealthwatch Management Console

As the management device, install the Stealthwatch Management Console at a location on your network that is accessible to all the devices sending data to it.

If you have a failover pair of Stealthwatch Management Consoles, we recommend installing the primary and the secondary consoles in separate physical locations. This strategy will enhance a disaster recovery effort should it become necessary.

Placing the Stealthwatch Flow Collector

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

When you place a Flow Collector outside a firewall, we recommend that you turn off the setting **Accept traffic from any exporter**.

Placing the Stealthwatch Flow Sensor

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

The Flow Sensor 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 the Stealthwatch UDP Director

The only requirement for the placement of the Stealthwatch UDP Director is that it has an unobstructed communication path to the rest of your Stealthwatch appliances.

If you are deploying UDP Director in an environment where [Cisco's ACI](#) is being utilized and Unicast Reverse Path Forwarding (uRPF) or **Limit IP learning to subnet** is enabled, the local network may block the forwarded traffic leaving the UDP Director. You need to spoof the UDP traffic as part of the forwarding rules so tools collecting the log data are able to know the original source of traffic.



To ensure a successful operation of the UDP Director in this case, deploy your UDP Director on a portion of your network where you can disable uRPF or **Limit IP learning to subnet** (typically internally). You can place the UDP Director in an L3 out (no IP learning). If on 4.0+, you can disable endpoint learning on a per VRF basis.

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
- TCP 5222
- UDP 53
- UDP 123
- UDP 161
- UDP 162
- UDP 389

- UDP 514
- UDP 2055
- UDP 6343

Communication Ports

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

From (Client)	To (Server)	Port	Protocol
Admin User PC	All appliances	TCP/443	HTTPS
All appliances	Network time source	UDP/123	NTP
Active Directory	Stealthwatch Management Console	TCP/389, UDP/389	LDAP
AnyConnect	Endpoint Concentrator	UDP/2055	NetFlow
Cisco ISE	Stealthwatch Management Console	TCP/443	HTTPS
Cisco ISE	Stealthwatch Management Console	TCP/5222	XMPP
Endpoint Concentrator	Flow Collector	UDP/2055	NetFlow
External log sources	Stealthwatch Management Console	UDP/514	SYSLOG
Flow Collector	Stealthwatch Management Console	TCP/443	HTTPS
SLIC	Stealthwatch Management Console	TCP/443 or proxied connection	HTTPS
UDP Director	Flow Collector - sFlow	UDP/6343	sFlow
UDP Director	Flow Collector - NetFlow	UDP/2055*	NetFlow
UDP Director	3rd Party event management systems	UDP/514	SYSLOG

From (Client)	To (Server)	Port	Protocol
Flow Sensor	Stealthwatch Management Console	TCP/443	HTTPS
Flow Sensor	Flow Collector - NetFlow	UDP/2055	NetFlow
Identity	Stealthwatch Management Console	TCP/2393	SSL
NetFlow Exporters	Flow Collector - NetFlow	UDP/2055*	NetFlow
sFlow Exporters	Flow Collector - sFlow	UDP/6343*	sFlow
Stealthwatch Management Console	Cisco ISE	TCP/443	HTTPS
Stealthwatch Management Console	DNS	UDP/53	DNS
Stealthwatch Management Console	Flow Collector	TCP/443	HTTPS
Stealthwatch Management Console	Flow Sensor	TCP/443	HTTPS
Stealthwatch Management Console	Identity	TCP/2393	SSL
Stealthwatch Management Console	Flow Exporters	UDP/161	SNMP
Stealthwatch Management Console	Endpoint Concentrator	UDP.2055	HTTPS
User PC	Stealthwatch Management Console	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
Stealthwatch Management Console	3rd Party event management	UDP/162	SNMP-trap
Stealthwatch Management Console	3rd Party event management	UDP/514	SYSLOG
Stealthwatch Management Console	Email gateway	TCP/25	SMTP
Stealthwatch Management Console	SLIC	TCP/443	SSL
User PC	All appliances	TCP/22	SSH

The following diagram shows the various connections used by Stealthwatch. The ports marked as optional are ones that may be used according to your own network needs.

Integrating the Flow Sensor into Your Network

The Stealthwatch Flow Sensor is versatile 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 needs.

Before you install a Flow Sensor, 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 Flow Sensor 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 Flow Sensor 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 Flow Sensor. The type of TAP you use depends on your network.

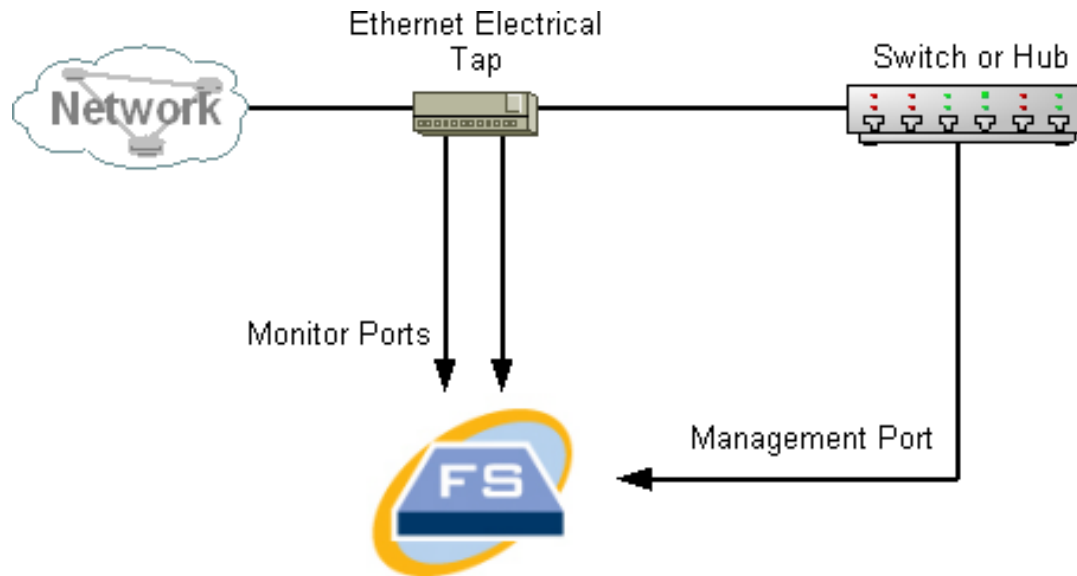
This section explains the following ways to use TAPs:

- **Using Electrical TAPs**
- **Using Optical TAPs**
- **Using TAPs Outside Your Firewall**
- **Placing the Flow Sensor Inside Your Firewall**

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

Using Electrical TAPs

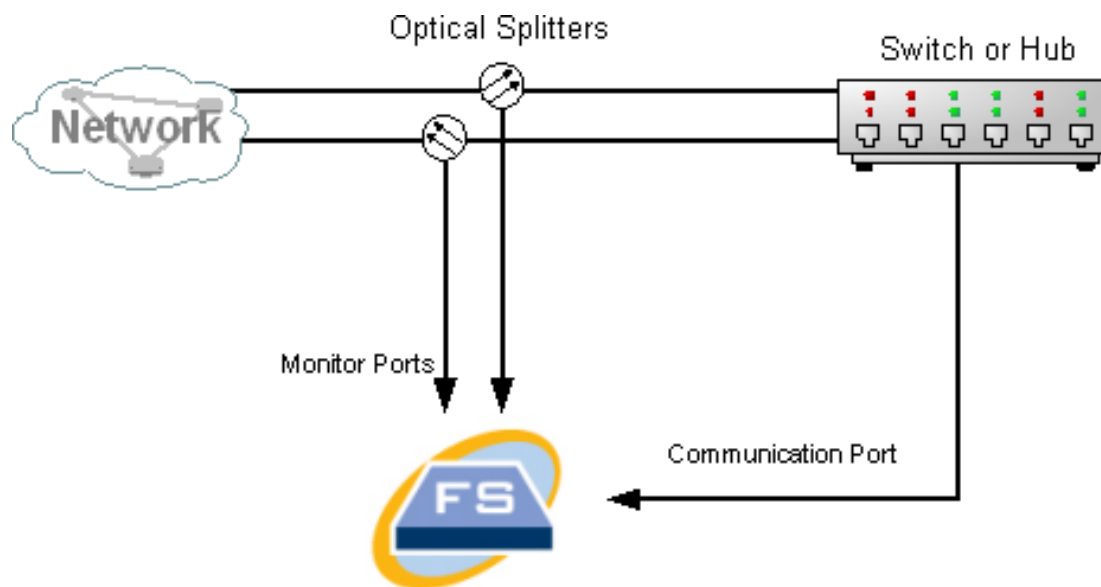
In the example below, the Flow Sensor is connected to an Ethernet electrical TAP. To do so, connect the two TAP ports to the Flow Sensor Monitor Ports 1 and 2.



Using Optical TAPs

Use two splitters for fiber-optic systems. Place a fiber-optic cable splitter in line with each transmission direction to repeat the optical signal for one transmission direction.

In the example below, the Flow Sensor is connected to a fiber-optic-based network. To do so, connect the outputs of the splitters to the Flow Sensor Monitor Ports 1 and 2.



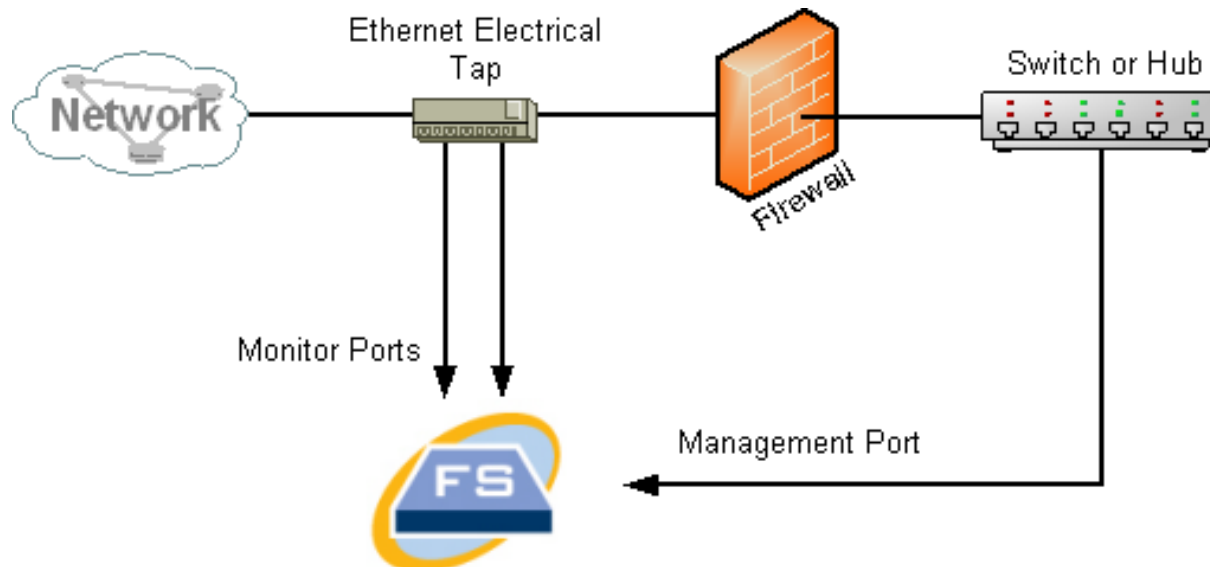
If the connection between the monitored networks is an optical connection, then the Flow Sensor is connected to two optical splitters. The management port is connected to either the switch of the monitored network or to another switch or hub.

Using TAPs Outside Your Firewall

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

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

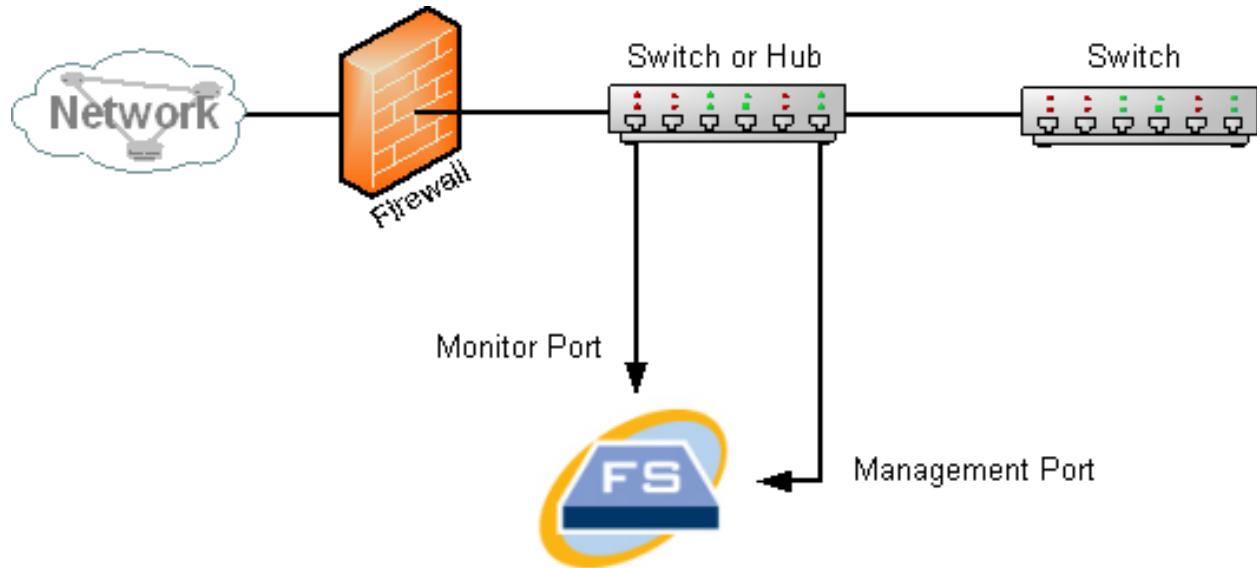
In the example below shows using an Ethernet electrical TAP. The management port must be connected to the switch or hub of the monitored network. This setup is similar to the setup that monitors traffic to and from your network.



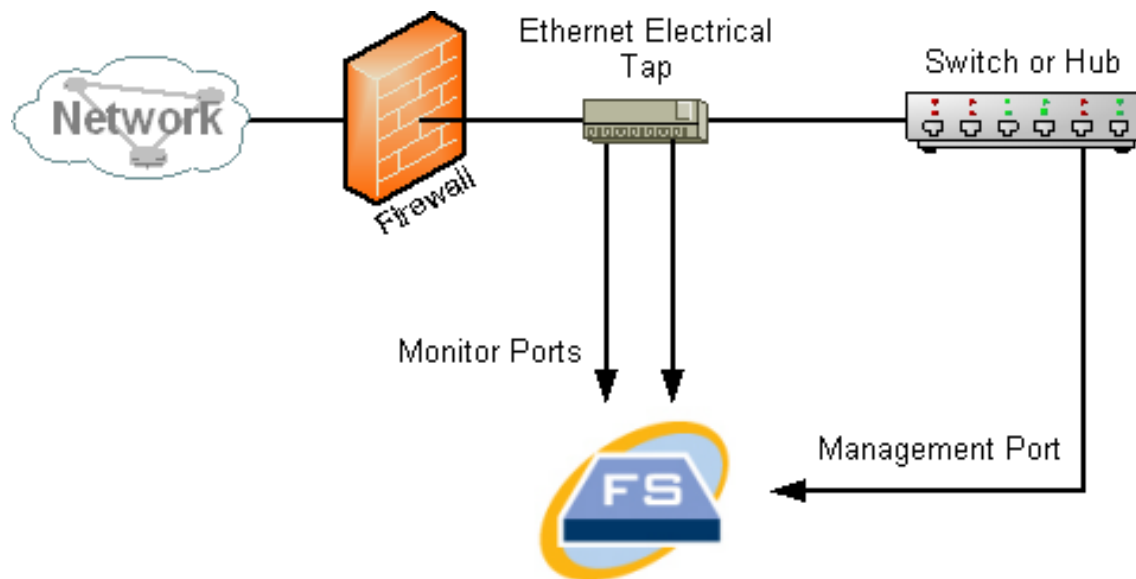
If your firewall is performing network address translation (NAT), you can observe only the addresses that are on the firewall.

Placing the Flow Sensor Inside Your Firewall

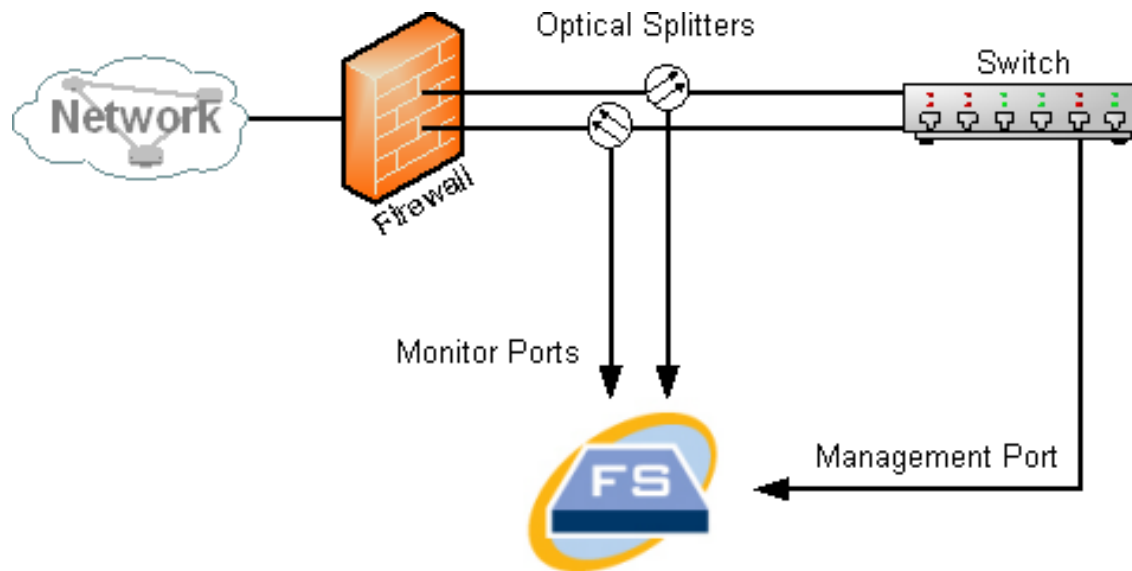
To monitor traffic between internal networks and a firewall, the Flow Sensor must be able to access all traffic between the firewall and the internal networks. You can accomplish this by configuring a mirror port that mirrors the connection to the firewall on the main switch. Make sure that the Flow Sensor 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.



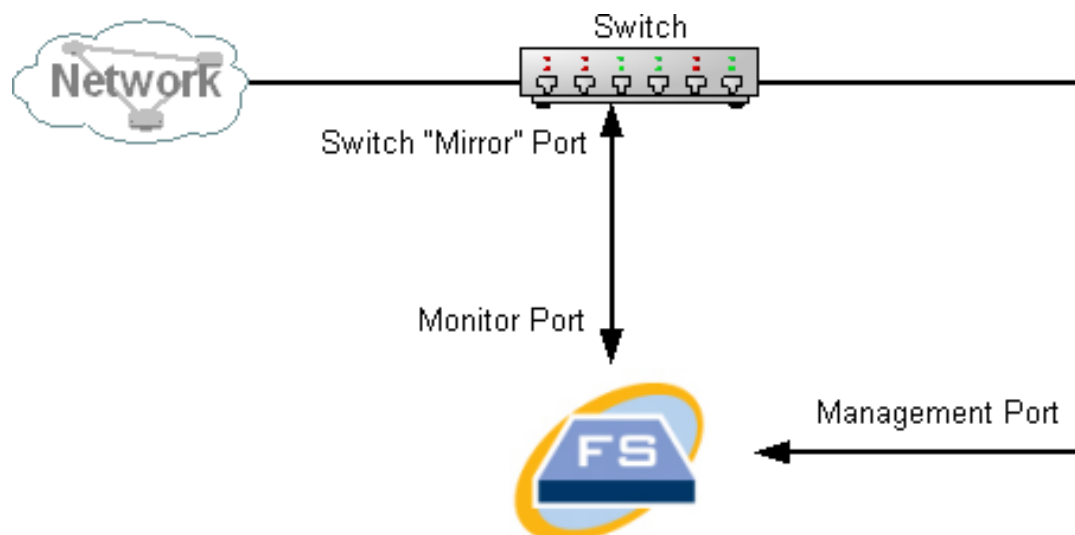
An optical splitter configuration is shown below.



SPAN Ports

You can also connect the Flow Sensor to a switch. However, because a switch does not repeat all traffic on each port, the Flow Sensor 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 Flow Sensor 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 Flow Sensor Monitor Port 1 must be connected to this mirror port. This allows the Flow Sensor 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 than physical connections of hosts. If the mirror port is configured to mirror all ports on a VLAN or switch, the Flow Sensor can monitor all traffic to, from, and within the network of interest, as well as other networks.

In all cases, we recommend 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.

Installation Preparation


Installation Warnings

Read the [Regulatory and Compliance Safety Information](#) document before installing the Stealthwatch x210 Series appliances.

Take note of the following warnings:


Statement 1071–Warning Definition

IMPORTANT SAFETY INSTRUCTIONS


 This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS


Statement 1005–Circuit Breaker

 This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than: USA: 120, 15 A (EU: 250V, 16A)

Statement 1004–Installation Instructions

 Read the installation instructions before using, installing or connecting the system to the power source.

Statement 12–Power Supply Disconnection Warning

 Before working on a chassis or working near power supplies, unplug the power cord on AC units; disconnect the power at the circuit breaker on DC units.

 Statement 43–Jewelry Removal Warning



Before working on equipment that is connected to power lines, remove jewelry (including rings, necklaces, and watches). Metal objects will heat up when connected to power and ground and can cause serious burns or weld the metal object to the terminals.

Statement 94–Wrist Strap Warning



During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the backplane with your hand or any metal tool, or you could shock yourself.

Statement 1045–Short-Circuit Protection



This product requires short-circuit (overcurrent) protection to be provided as part of the building installation. Install only in accordance with national and local wiring regulations.

Statement 1021–SELV Circuit



To avoid electric shock, do not connect safety extra-low voltage (SELV) circuits to telephone-network voltage (TNV) circuits. LAN ports contain SELV circuits, and WAN ports contain TNV circuits. Some LAN and WAN ports both use RJ-45 connectors. Use caution when connecting cables.

Statement 1024–Ground Conductor



This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.

Statement 1040–Product Disposal



Ultimate disposal of this product should be handled according to all national laws and regulations.

Statement 1074—Comply with Local and National Electrical Codes

Installation of the equipment must comply with local and national electrical codes.

Statement 19—TN Power Warning

The device is designed to work with TN power systems.

Installation Guidelines

Take note of the following warnings:

Statement 1047—Overheating Prevention

To prevent the system from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of : 41 to 95° F (5 to 35° C)

Statement 1019—Main Disconnecting Device

The plug-socket combination must be accessible at all times, because it serves as the main disconnecting device.

Statement 1005—Circuit Breaker

This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than: USA: 120, 15 A (EU: 250 V, 16 A)

Statement 1074—Comply with Local and National Electrical Codes

Installation of the equipment must comply with local and national electrical codes.

Statement 371—Power Cable and AC Adapter

When installing the product, please use the provided or designated connection cables/power cables/AC adaptors/batteries. Using any other cables/adaptors



could cause a malfunction or a fire. Electrical Appliance and Material Safety Law prohibits the use of UL-certified cables (that have the "UL" or "CSA" shown on the cord), not regulated with the subject law by showing "PSE" on the cord, for any other electrical devices than products designated by CISCO.



Statement 1073—No User-Serviceable Parts

No user-serviceable parts inside. Do not open.

When you are installing a chassis, use the following guidelines:

- Ensure that there is adequate space around the chassis to allow for servicing and for adequate airflow. The airflow in the chassis is from front to back.



To ensure proper airflow it is necessary to rack your chassis using rail kits. Physically placing the units on top of one another or stacking without the use of the rail kits blocks the air vents on top of the chassis, which could result in overheating, higher fan speeds, and higher power consumption. We recommend that you mount your chassis on rail kits when you are installing them into the rack because these rails provide the minimal spacing required between the chassis. No additional spacing between the chassis is required when you mount them using rail kits.

- Ensure that the air-conditioning can keep the chassis at a temperature of 41 to 95° F (5 to 35° C).
- Ensure that the cabinet or rack meets the rack requirements.
- Ensure that the site power meets the power requirements listed in the [specification sheet](#) for your appliance. If available, you can use a UPS to protect against power failures.



Avoid UPS types that use ferroresonant technology. These UPS types can become unstable with these systems, which can have substantial current draw fluctuations from fluctuating data traffic patterns.

Safety Recommendations

The following information helps to ensure your safety and to protect the chassis. This information may not address all potentially hazardous situations in your working environment, so be alert and exercise good judgment at all times.

Observe these safety guidelines:

- Keep the area clear and dust free before, during, and after installation.
- Keep tools away from walkways, where you and others might trip over them.
- Do not wear loose clothing or jewelry, such as earrings, bracelets, or chains that could get caught in the chassis.
- Wear safety glasses if you are working under any conditions that might be hazardous to your eyes.
- Do not perform any action that creates a potential hazard to people or makes the equipment unsafe.
- Never attempt to lift an object that is too heavy for one person.

Maintain Safety with Electricity

 Before working on a chassis, be sure the power cord is unplugged.

Follow these guidelines when working on equipment powered by electricity:

- Do not work alone if potentially hazardous conditions exist anywhere in your work space.
- Never assume that power is disconnected; always check.
- Look carefully for possible hazards in your work area, such as moist floors, ungrounded power extension cables, frayed power cords, and missing safety grounds.
- If an electrical accident occurs:
 - Use caution; do not become a victim yourself.
 - Disconnect power from the system.
 - If possible, send another person to get medical aid. Otherwise, assess the condition of the victim, and then call for help.
 - Determine whether the person needs rescue breathing or external cardiac compressions; then take appropriate action.
- Use the chassis within its marked electrical ratings and product usage instructions.

Prevent ESD Damage

ESD occurs when electronic components are improperly handled, and it can damage equipment and impair electrical circuitry, which can result in intermittent or complete failure of your equipment.

Always follow ESD-prevention procedures when removing and replacing components. Ensure that the chassis is electrically connected to an earth ground. Wear an ESD-preventive wrist strap, ensuring that it makes good skin contact. Connect the grounding clip to an unpainted surface of the chassis frame to safely ground ESD voltages. To properly guard against ESD damage and shocks, the wrist strap and cord must operate effectively. If no wrist strap is available, ground yourself by touching the metal part of the chassis.

For safety, periodically check the resistance value of the antistatic strap, which should be between one and 10 megohms.

Site Environment

To avoid equipment failures and reduce the possibility of environmentally caused shutdowns, plan the site layout and equipment locations carefully. If you are currently experiencing shutdowns or unusually high error rates with your existing equipment, these considerations may help you isolate the cause of failures and prevent future problems.

Power Supply Considerations

When installing the chassis, consider the following:

- Check the power at the site before installing the chassis to ensure that it is free of spikes and noise. Install a power conditioner, if necessary, to ensure proper voltages and power levels in the appliance-input voltage.
- Install proper grounding for the site to avoid damage from lightning and power surges.
- The chassis does not have a user-selectable operating range. Refer to the label on the chassis for the correct appliance input-power requirement.
- Several styles of AC-input power supply cords are available for the appliance; make sure that you have the correct style for your site.
- If you are using dual redundant (1+1) power supplies, we recommend that you use independent electrical circuits for each power supply.
- Install an uninterruptible power source for your site, if possible.

Rack Configuration Considerations

Consider the following when planning a rack configuration:

- If you are mounting a chassis in an open rack, make sure that the rack frame does not block the intake or exhaust ports.
- Be sure enclosed racks have adequate ventilation. Make sure that the rack is not overly congested as each chassis generates heat. An enclosed rack should have louvered sides and a fan to provide cooling air.
- In an enclosed rack with a ventilation fan in the top, heat generated by equipment near the bottom of the rack can be drawn upward and into the intake ports of the equipment above it in the rack. Ensure that you provide adequate ventilation for equipment at the bottom of the rack.
- Baffles can help to isolate exhaust air from intake air, which also helps to draw cooling air through the chassis. The best placement of the baffles depends on the air-flow patterns in the rack. Experiment with different arrangements to position the baffles effectively.

Installation

This section covers installing your appliances in your environment. It includes:

- **Mounting Your Appliance**
- **Connecting Your Appliance to the Network**
- **Connecting to Your Appliance**
- **Changing Default Information**

Mounting Your Appliance

You can mount Stealthwatch appliances directly in a standard 19" rack or cabinet, any other suitable cabinet, or on a flat surface. 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 appliances:

- AC power cord
- Access keys (for front face plate)
- Rail kit for rack mounting or mounting ears for smaller appliances
- For the Flow Collector 5210, a 10 GB SFP cable

Additional Required Hardware

You must provide the following additional required hardware:

- Mounting screw for a standard 19" rack
- Uninterruptible power supply (UPS) for each appliance you are installing
- 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

Connecting Your Appliance to the Network

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

For detailed specification information about each appliance, refer to [Stealthwatch Specification Sheets](#).



The Cisco x210 hardware all use the same UCS platform, UCSC-C220-M5SX, except for the Flow Collector 5210 DB, which uses UCSC-C240-M5SX. The variations in appliances are in NIC cards, processor, memory, storage and RAID.



The Flow Collector 5210 consists of two connected servers (engine and database) so they function as a single appliance. Because of this, the installation slightly differs from other appliances. First, connect them together directly by a 10G SFP+ DA Cross Connect cable. Then, connect to your network.

To connect your appliance to your network:

1. Connect an Ethernet cable to the management port, at the rear of the appliance.
2. Connect at least one monitor port for Flow Sensors and UDP Directors.

For the UDP Director HA, connect the two UDP Directors by crossover cables. Connect the eth2 port of one UDP Director 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.

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.

Connecting to Your Appliance

This section describes how to connect to your appliance in order to change the default user passwords.

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

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


For new appliances, 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. Wait for it to finish booting up completely. Do not interrupt the boot up process.

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 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 Default Information](#).

Connecting with a Laptop

You can also connect to the appliance with a laptop that has a terminal emulator.

To connect to an appliance with a laptop:

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

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 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.

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

5. Apply the following the settings:

- BPS: 115200
- 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 Default Information](#).

Changing Default Information

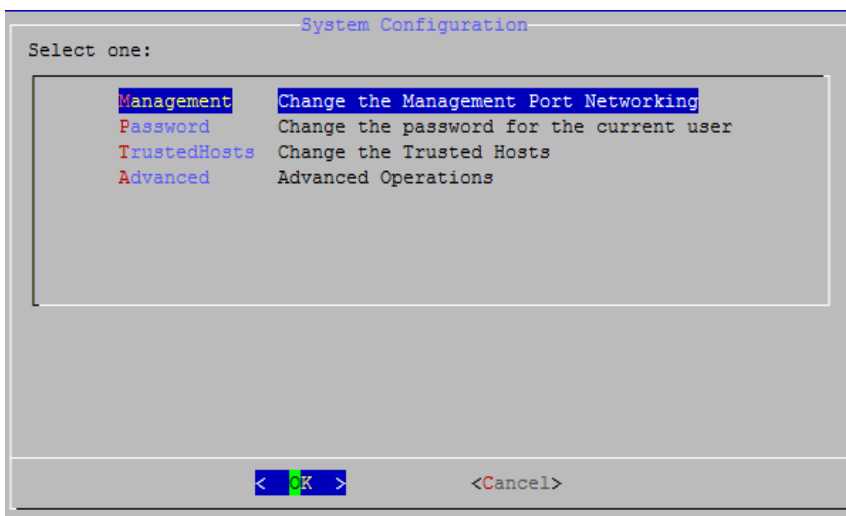
After you have connected to the appliance, configure the IP addresses and change the user passwords.

Changing the Default IP Addresses

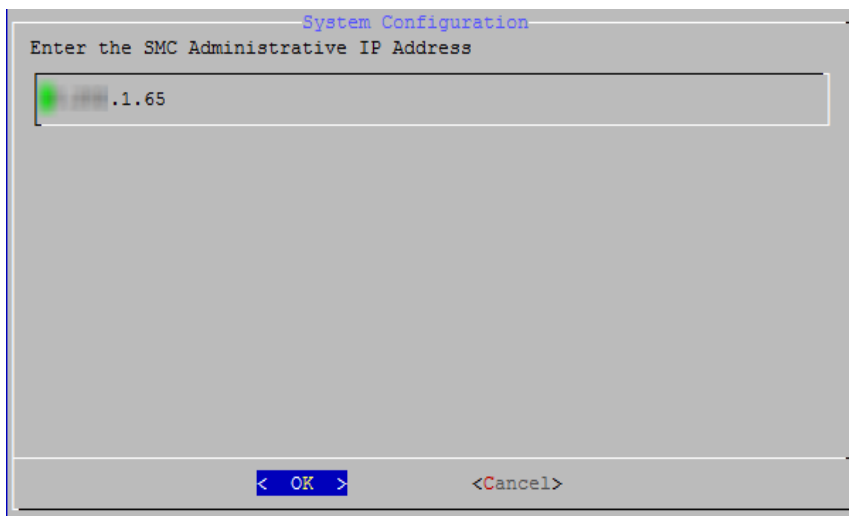
The appliances already have default IP addresses, but configure them for your network.

1. Log in to the System Configuration program:
 - 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.



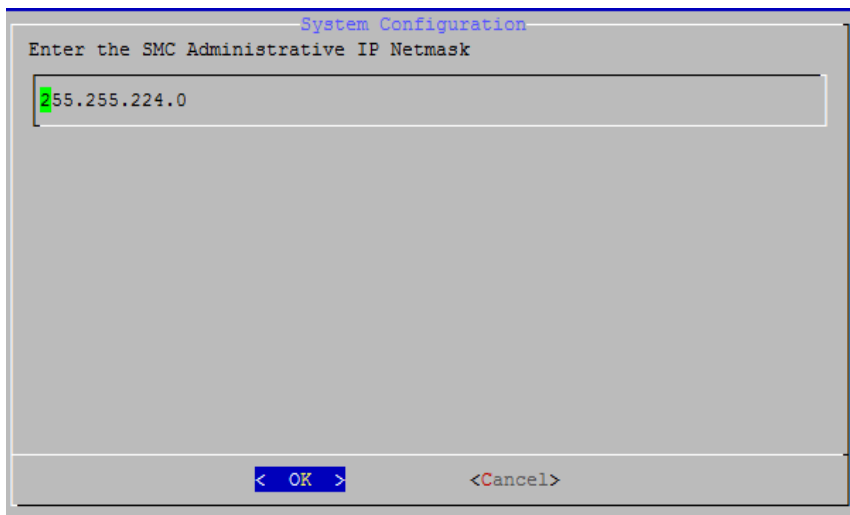
2. Select **Management**, and then press **Enter**. The IP Address page opens.



The screenshot shows a dialog box titled "System Configuration" with the prompt "Enter the SMC Administrative IP Address". A text input field contains the value ".1.65". At the bottom of the dialog, there are two buttons: "< OK >" and "<Cancel>".

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

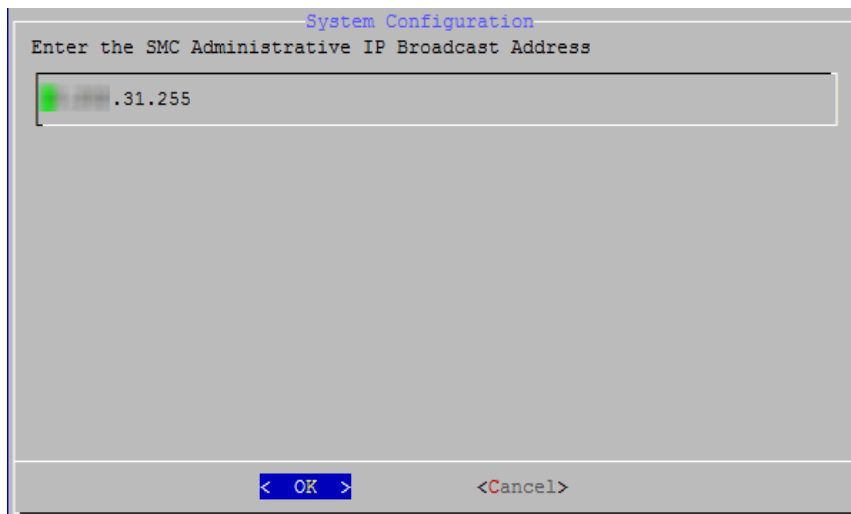
The IP netmask page opens with the default value.



The screenshot shows a dialog box titled "System Configuration" with the prompt "Enter the SMC Administrative IP Netmask". A text input field contains the value "55.255.224.0". At the bottom of the dialog, there are two buttons: "< OK >" and "<Cancel>".

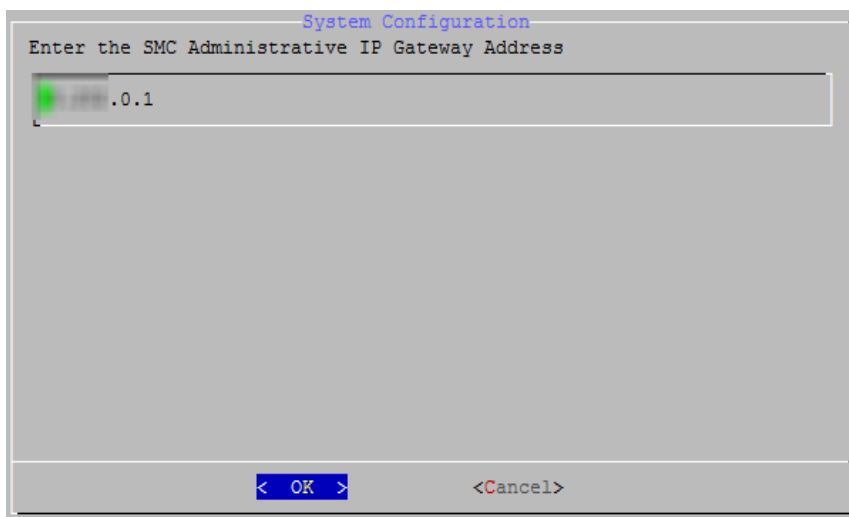
4. Accept the default value or enter a new IP Netmask address based on your environment. Select **OK**, and then press **Enter** to continue.

The Broadcast Address page opens.



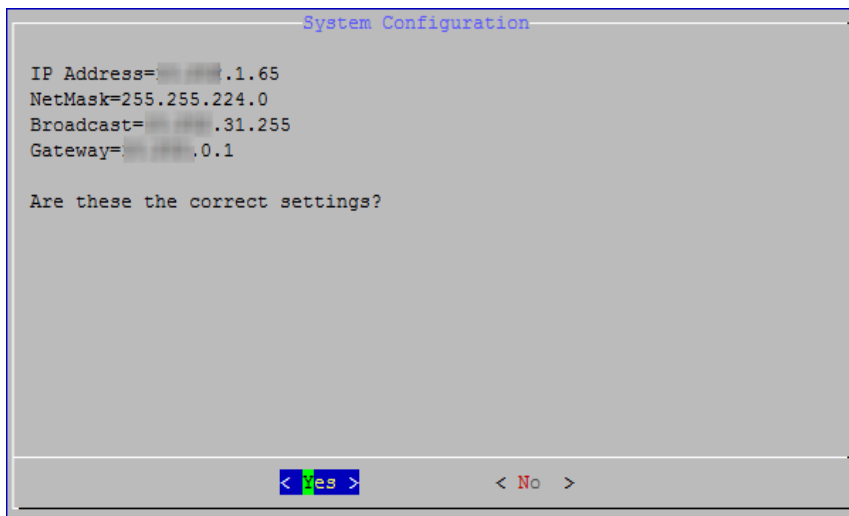
5. Accept the default value or enter a new one based on your environment. Select **OK**, and then press **Enter** to continue.

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



6. 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.



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, [Changing the Sysadmin User Password](#) .

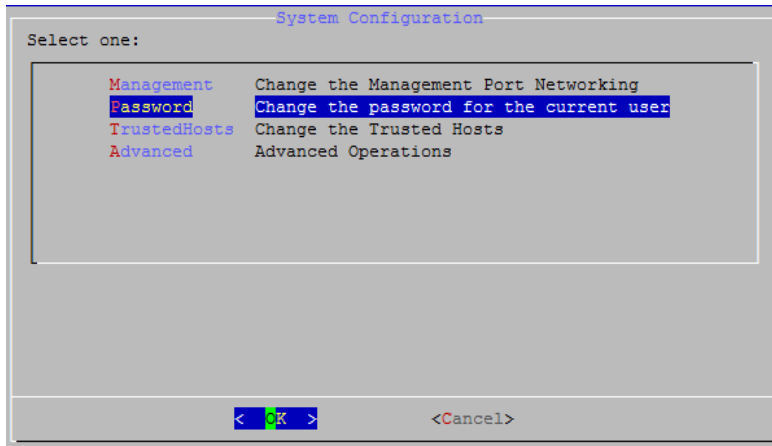
Changing the Sysadmin User Password

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

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

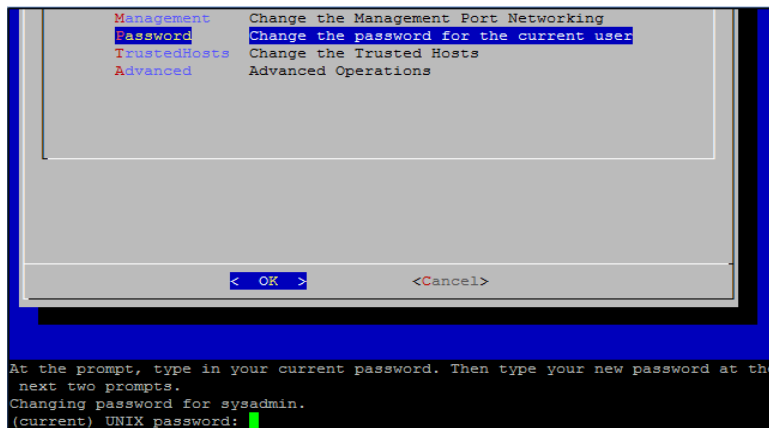
To change the sysadmin password:

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



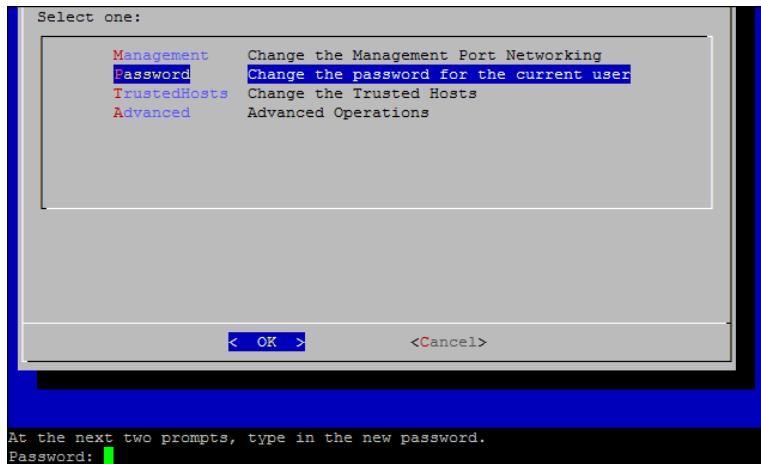
If you change the trusted hosts list from the defaults, make sure each Stealthwatch appliance is included in the trusted host list for every other Stealthwatch appliance in your deployment. Otherwise, the appliances will not be able to communicate with each other.

A prompt for the current password appears below the menu.



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

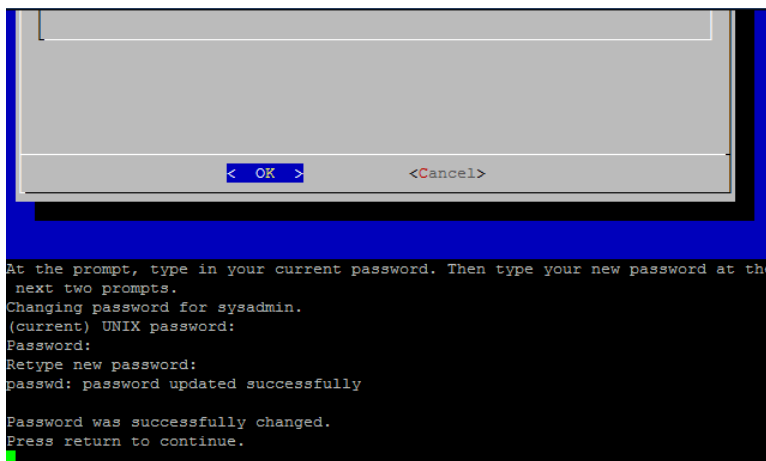
The prompt for a new password appears.



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

The password must be between 8 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**.

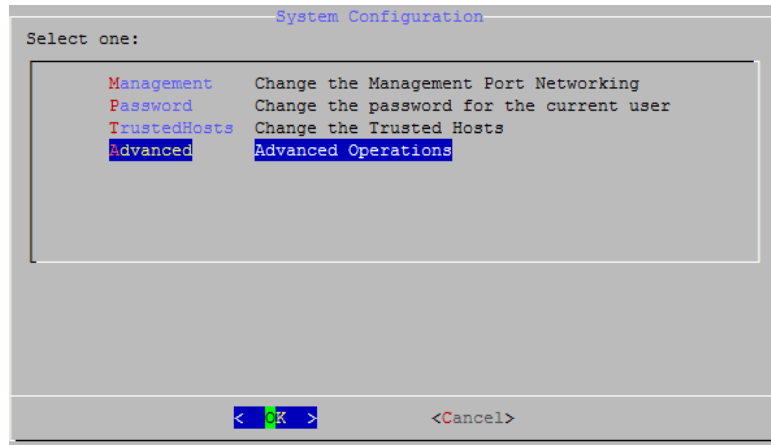


5. When your password is accepted, press **Enter** again to return to the System Configuration menu.
6. Continue with the next section, [Changing the Root User Password](#).

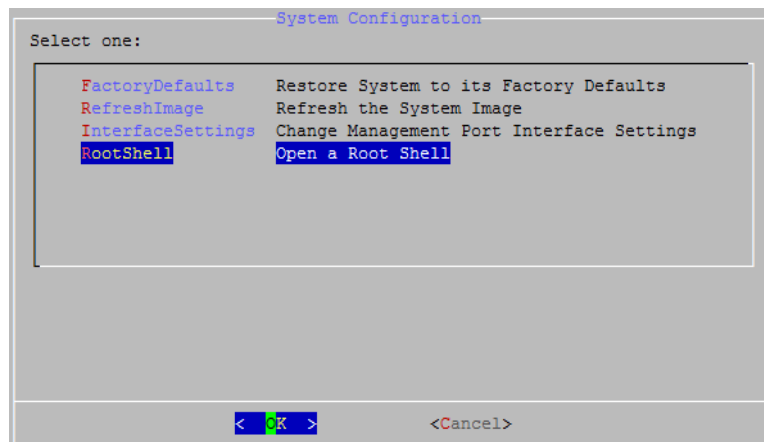
Changing the Root User Password

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

1. Go to go to the root shell.

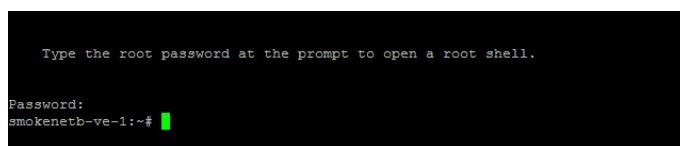


2. On the System Configuration menu, select **Advanced**, and then press **Enter**. The Advanced menu appears.



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

A prompt for the root password appears.



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.

```

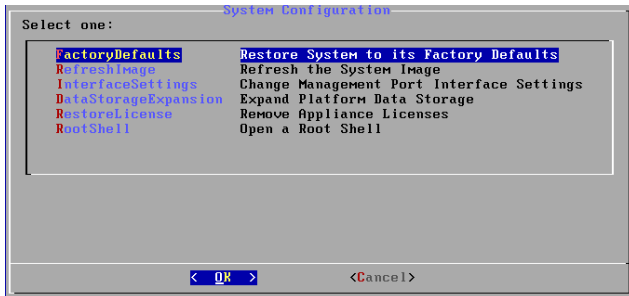
  < OK >      <Cancel>

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

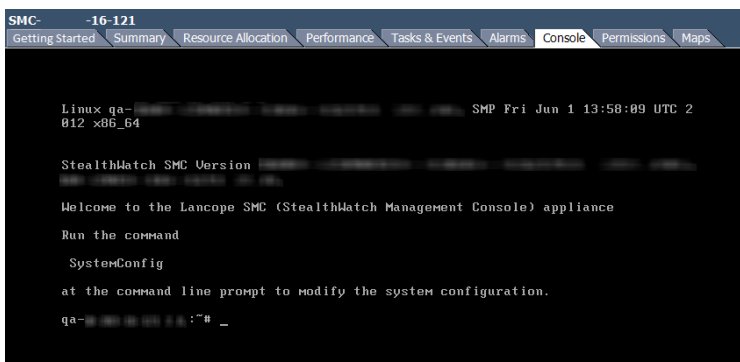
Password was successfully changed.
Press return to continue.
█

```


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.



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



11. Type **exit** and press **Enter**. The login prompt appears.
12. Press **Ctrl+Alt** to exit the Console environment.

Configuring Your Appliance

You are now ready to configure your appliance. To configure your appliance, refer to the applicable [Stealthwatch Installation and Configuration Guide](#) for your software version. The x210 Series is compatible with Stealthwatch 7.x software versions.

Copyright Information

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

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

