



STONEGATE 5.2

INSTALLATION GUIDE

INTRUSION PREVENTION SYSTEM

STONESOFT

Secure Information Flow

Legal Information

End-User License Agreement

The use of the products described in these materials is subject to the then current end-user license agreement, which can be found at the Stonesoft website:

www.stonesoft.com/en/support/eula.html

Third Party Licenses

The StoneGate software includes several open source or third-party software packages. The appropriate software licensing information for those products at the Stonesoft website:

www.stonesoft.com/en/support/third_party_licenses.html

U.S. Government Acquisitions

If Licensee is acquiring the Software, including accompanying documentation on behalf of the U.S. Government, the following provisions apply. If the Software is supplied to the Department of Defense ("DoD"), the Software is subject to "Restricted Rights", as that term is defined in the DOD Supplement to the Federal Acquisition Regulations ("DFAR") in paragraph 252.227-7013(c) (1). If the Software is supplied to any unit or agency of the United States Government other than DOD, the Government's rights in the Software will be as defined in paragraph 52.227-19(c) (2) of the Federal Acquisition Regulations ("FAR"). Use, duplication, reproduction or disclosure by the Government is subject to such restrictions or successor provisions.

Product Export Restrictions

The products described in this document are subject to export control under the laws of Finland and the European Council Regulation (EC) N:o 1334/2000 of 22 June 2000 setting up a Community regime for the control of exports of dual-use items and technology (as amended). Thus, the export of this Stonesoft software in any manner is restricted and requires a license by the relevant authorities.

General Terms and Conditions of Support and Maintenance Services

The support and maintenance services for the products described in these materials are provided pursuant to the general terms for support and maintenance services and the related service description, which can be found at the Stonesoft website:

www.stonesoft.com/en/support/view_support_offering/terms/

Replacement Service

The instructions for replacement service can be found at the Stonesoft website:

www.stonesoft.com/en/support/view_support_offering/return_material_authorization/

Hardware Warranty

The appliances described in these materials have a limited hardware warranty. The terms of the hardware warranty can be found at the Stonesoft website:

www.stonesoft.com/en/support/view_support_offering/warranty_service/

Trademarks and Patents

The products described in these materials are protected by one or more of the following European and US patents: European Patent Nos. 1065844, 1189410, 1231538, 1259028, 1271283, 1289183, 1289202, 1304849, 1313290, 1326393, 1379046, 1330095, 131711, 1317937 and 1443729 and US Patent Nos. 6,650,621; 6,856,621; 6,885,633; 6,912,200; 6,996,573; 7,099,284; 7,127,739; 7,130,266; 7,130,305; 7,146,421; 7,162,737; 7,234,166; 7,260,843; 7,280,540; 7,302,480; 7,386,525; 7,406,534; 7,461,401; 7,721,084; and 7,739,727 and may be protected by other EU, US, or other patents, or pending applications. Stonesoft, the Stonesoft logo and StoneGate, are all trademarks or registered trademarks of Stonesoft Corporation. All other trademarks or registered trademarks are property of their respective owners.

Disclaimer

Although every precaution has been taken to prepare these materials, THESE MATERIALS ARE PROVIDED "AS-IS" and Stonesoft makes no warranty to the correctness of information and assumes no responsibility for errors, omissions, or resulting damages from the use of the information contained herein. All IP addresses in these materials were chosen at random and are used for illustrative purposes only.

Copyright © 2011 Stonesoft Corporation. All rights reserved. All specifications are subject to change.

TABLE OF CONTENTS

INTRODUCTION

CHAPTER 1

Using StoneGate Documentation	7
How to Use This Guide	8
Documentation Available	9
Product Documentation	9
Support Documentation	9
System Requirements	10
Supported Features	10
Contact Information	10
Licensing Issues	10
Technical Support	10
Your Comments	10
Other Queries	10

PREPARING FOR INSTALLATION

CHAPTER 2

Planning the IPS Installation	13
Introduction to StoneGate IPS	14
Example Network Scenario	14
Overview to the Installation Procedure	15
Important to Know Before Installation	15
Supported Platforms	15
Date and Time Settings	15
Capture Interfaces	16
Switch SPAN Ports	16
Network TAPs	16
Cabling Guidelines	16
Speed And Duplex	17
Installing IPS Licenses	19

CHAPTER 3

Getting Started with IPS Licenses	20
Configuration Overview	20
Generating New Licenses	20
Installing Licenses	21

CHAPTER 4

Configuring NAT Addresses	23
Getting Started with NAT Addresses	24
Configuration Overview	25
Defining Locations	25
Adding SMC Server Contact Addresses	26

CONFIGURING SENSORS AND ANALYZERS

CHAPTER 5

Defining Sensors and Analyzers	31
Getting Started with Defining Sensors and Analyzers	32
Creating Engine Elements	32
Defining System Communication Interfaces for IPS Engines	33
Defining Physical Interfaces	34
Defining VLAN Interfaces	35
Defining IP Addresses	36
Setting Interface Options for IPS Engines	37
Defining Traffic Inspection Interfaces for Sensors	38
Defining Logical Interfaces	39
Defining Reset Interfaces	40
Defining Capture Interfaces	41
Defining Inline Interfaces	42
Bypassing Traffic on Overload	43
Finishing the Engine Configuration	44

CHAPTER 6

Saving the Initial Configuration	45
Configuration Overview	46
Saving the Initial Configuration for Sensors and Analyzers	46
Transferring the Initial Configuration to Sensors and Analyzers	49

CHAPTER 7

Configuring Routing and Installing Policies	51
Configuring Routing	52
Adding Next-hop Routers	53
Adding the Default Route	54
Adding Other Routes	54
Installing the Initial Policy	55
Commanding IPS Engines	57

INSTALLING SENSORS AND ANALYZERS

CHAPTER 8

Installing the Engine on Intel-Compatible Platforms	61
Installing the Sensor or Analyzer Engine	62
Configuration Overview	62
Obtaining Installation Files	62

Downloading the Installation Files	62
Checking File Integrity	62
Creating the Installation CD-ROM	63
Starting the Installation	63
Configuring the Engine	64
Configuring the Engine Automatically with a USB Stick	64
Configuring the Engine in the Engine Configuration Wizard	65
Configuring the Operating System Settings	65
Configuring the Network Interfaces	67
Contacting the Management Server	68
Activating the Initial Configuration	68
Filling in the Management Server Information	69
Selecting the Engine Type	69
After Successful Management Server Contact	70
Installing the Engine in Expert Mode	70
Partitioning the Hard Disk Manually	70
Allocating Partitions	71

UPGRADING

CHAPTER 9	
Upgrading	75
Getting Started with Upgrading	76
Configuration Overview	77
Obtaining Installation Files	77
Upgrading or Generating Licenses	78
Upgrading Licenses Under One Proof Code	78
Upgrading Licenses Under Multiple Proof Codes	79
Installing Licenses	80
Checking the Licenses	81
Upgrading Engines Remotely	82
Upgrading Engines Locally	84
Upgrading from an Engine Installation CD-ROM	84
Upgrading from a ZIP Archive File	85

APPENDICES

APPENDIX A	
Command Line Tools	89
StoneGate-Specific Commands	90
General Tools	93

APPENDIX B	
Default Communication Ports	95
Management Center Ports	96
IPS Engine Ports	98
APPENDIX C	
Example Network Scenario	101
Overview of the Example Network	102
Example Headquarters Intranet Network	103
HQ Sensor Cluster	103
Example Headquarters Management Network	104
HQ Analyzer	104
HQ Firewall	104
Management Center Servers	104
Example Headquarters DMZ Network	105
DMZ Sensor	105
Example Branch Office Network	106
Branch Office Sensor-Analyzer	106
Branch Office Firewall	106
Branch Office Log Server	106
Index	107

INTRODUCTION

In this section:

[Using StoneGate Documentation - 7](#)

CHAPTER 1

USING STONEGATE DOCUMENTATION

Welcome to Stonesoft's StoneGate™ IPS. This chapter describes how to use the *StoneGate IPS Installation Guide* and lists other available documentation. It also provides directions for obtaining technical support and giving feedback.

The following sections are included:

- ▶ [How to Use This Guide](#) (page 8)
- ▶ [Documentation Available](#) (page 9)
- ▶ [Contact Information](#) (page 10)

How to Use This Guide

This *IPS Installation Guide* is intended for administrators who install the StoneGate IPS system. It describes the IPS Sensor and Analyzer engine installation step by step. The chapters in this guide are organized in the general order you should follow when installing the system.

Most tasks are explained using illustrations that include explanations on the steps you need to complete in each corresponding view in your own environment. The explanations that accompany the illustrations are numbered when the illustration contains more than one step for you to perform.

Typographical Conventions

The following conventions are used throughout the documentation:

Table 1.1 Typographical Conventions

Formatting	Informative Uses
User Interface text	Text you see in the User Interface (buttons, menus, etc.) and any other interaction with the user interface are in bold-face .
<i>References, terms</i>	Cross-references and first use of acronyms and terms are in <i>italics</i> .
Command line	File names, directories, and text displayed on the screen are monospaced.
User input	User input on screen is in monospaced bold-face .
<i>Command parameters</i>	Command parameter names are in <i>monospaced italics</i> .

We use the following ways to indicate important or additional information:



Note – Notes prevent commonly-made mistakes by pointing out important points.



Caution – Cautions prevent breaches of security, information loss, or system downtime. Cautions always contain critical information that you must observe.

Tip – Tips provide additional helpful information, such as alternative ways to complete steps.

Example Examples present a concrete scenario that clarifies the points made in the adjacent text.

Documentation Available

StoneGate documentation is divided into two main categories: [Product Documentation](#) and [Support Documentation](#). Each StoneGate product has a separate set of manuals.

Product Documentation

The table below lists the available product documentation. PDF guides are available on the Management Center CD-ROM and at <http://www.stonesoft.com/support/>.

Table 1.2 Product Documentation

Guide	Description
Reference Guide	Explains the operation and features of StoneGate comprehensively. Demonstrates the general workflow and provides example scenarios for each feature area. Available for StoneGate Management Center, Firewall/VPN, and StoneGate IPS.
Installation Guide	Instructions for planning, installing, and upgrading a StoneGate system. Available for StoneGate Management Center, Firewall/VPN, and IPS.
Online Help	Describes how to configure and manage the system step-by-step. Accessible through the Help menu and by using the Help button or the F1 key in any window or dialog. Available in the StoneGate Management Client and the StoneGate Web Portal. An HTML-based system is available in the StoneGate SSL VPN Administrator through help links and icons.
Administrator's Guide	Describes how to configure and manage the system step-by-step. Available as a combined guide for both StoneGate Firewall/VPN and StoneGate IPS, and as separate guides for StoneGate SSL VPN and StoneGate IPsec VPN Client.
User's Guide	Instructions for end-users. Available for the StoneGate IPsec VPN Client and the StoneGate Web Portal.
Appliance Installation Guide	Instructions for physically installing and maintaining StoneGate appliances (rack mounting, cabling, etc.). Available for all StoneGate hardware appliances.

Support Documentation

The StoneGate support documentation provides additional and late-breaking technical information. These technical documents support the StoneGate Guide books, for example, by giving further examples on specific configuration scenarios.

The latest StoneGate technical documentation is available at the Stonesoft website at <http://www.stonesoft.com/support/>.

System Requirements

The certified platforms for running StoneGate engine software can be found at the product pages at http://www.stonesoft.com/en/products/ips/Software_Solutions/.

The hardware and software requirements for the version of StoneGate you are running can also be found in the [Release Notes](#) available at the StoneGate Support Documentation pages.

Supported Features

Not all StoneGate features are supported on all platforms. See the [Appliance Software Support Table](#) at the Stonesoft Support Documentation pages for more information.

Contact Information

For street addresses, phone numbers, and general information about StoneGate and Stonesoft Corporation, visit our website at <http://www.stonesoft.com/>.

Licensing Issues

You can view your current licenses at the License Center section of the Stonesoft website at <https://my.stonesoft.com/managelicense.do>.

For license-related queries, e-mail order@stonesoft.com.

Technical Support

Stonesoft offers global technical support services for Stonesoft's product families. For more information on technical support, visit the Support section at the Stonesoft website at <http://www.stonesoft.com/support/>.

Your Comments

We want to make our products fulfill your needs as well as possible. We are always pleased to receive any suggestions you may have for improvements.

- To comment on software and hardware products, e-mail feedback@stonesoft.com.
- To comment on the documentation, e-mail documentation@stonesoft.com.

Other Queries

For queries regarding other matters, e-mail info@stonesoft.com.

PREPARING FOR INSTALLATION

In this section:

Planning the IPS Installation - 13

Installing IPS Licenses - 19

Configuring NAT Addresses - 23

CHAPTER 2

PLANNING THE IPS INSTALLATION

This chapter provides important information to take into account before the installation can begin. The chapter also includes an overview to the installation process.

The following sections are included:

- ▶ [Introduction to StoneGate IPS](#) (page 14)
- ▶ [Example Network Scenario](#) (page 14)
- ▶ [Overview to the Installation Procedure](#) (page 15)
- ▶ [Important to Know Before Installation](#) (page 15)
- ▶ [Capture Interfaces](#) (page 16)

Introduction to StoneGate IPS

A StoneGate IPS system consists of Sensors, Analyzers, and the StoneGate Management Center. Sensors pick up network traffic, inspect it, and create event data for further processing by the Analyzers.

StoneGate Sensors and Analyzers can be distributed as follows:

- a combined Sensor-Analyzer with these two components on a single machine.
- a single node Sensor.
- a Sensor cluster, which consists of 2 to 16 machines with Sensors called *cluster nodes* or *nodes* for short.
- an Analyzer, which is required when a single node Sensor or a Sensor cluster is used.

You can install sensors in two basic ways:

- IDS (intrusion detection system) installation: Sensors capture and inspect all traffic in the connected network segment, but do not, by default, interrupt the flow of traffic in any way.
- IPS (intrusion prevention system) installation: Sensors are installed inline, so that all traffic that is to be inspected flows through the Sensor. In this setup, the Sensor itself can also be used to automatically block selected traffic according to how you configure it. Inline sensors in transparent access control mode (requires a separate license) provide transparent access control and logging for Ethernet (layer 2) traffic.

The main features of StoneGate IPS include:

- Multiple detection methods: misuse detection uses fingerprints to detect known attacks. Anomaly detection uses traffic statistics to detect unusual network behavior. Protocol validation identifies violations of the defined protocol for a particular type of traffic. Event correlation in the Analyzer processes event information received from the Sensors to detect a pattern of events that might indicate an intrusion attempt.
- Response mechanisms: There are several response mechanisms to anomalous traffic. These include different alerting channels, traffic recording, TCP connection termination, traffic blacklisting, and traffic blocking with inline IPS.

The sensors and analyzers are always managed centrally through the StoneGate Management Center (SMC). You must have an SMC configured before you can proceed with installing the sensors and analyzers. The SMC can be used to manage a large number of different StoneGate products. The SMC installation is covered in a separate guide. See the *SMC Reference Guide* for more background information on the SMC, and the *IPS Reference Guide* for more background information on the StoneGate sensors and analyzers.

Example Network Scenario

To get a better understanding of how StoneGate fits into a network, you can consult the Example Network Scenario that shows you one way to deploy StoneGate. See [Example Network Scenario](#) (page 101).

Overview to the Installation Procedure

1. Check the surrounding network environment as explained in [Capture Interfaces](#) (page 16).
2. Install licenses for the IPS engines. See [Installing IPS Licenses](#) (page 19).
3. If network address translation (NAT) is applied to communications between system components and the IPS engines, define Contact Addresses. See [Configuring NAT Addresses](#) (page 23).
4. Define the Sensor and Analyzer element(s) in the Management Client. See [Defining Sensors and Analyzers](#) (page 31).
5. Generate the initial configuration for the sensor and analyzer engine(s). See [Saving the Initial Configuration](#) (page 45).
6. Install and configure the sensors and analyzers.
 - For hardware installation and initial configuration of StoneGate appliances, see the *Appliance Installation Guide* that is delivered with each appliance.
 - For software installations, see [Installing the Engine on Intel-Compatible Platforms](#) (page 61).
7. Configure routing and install a policy on the sensor(s). See [Configuring Routing and Installing Policies](#) (page 51).

The chapters and sections of this guide proceed in the order outlined above.

Important to Know Before Installation

Before you start the installation, you need to carefully plan the site that you are going to install. Consult the *Reference Guide* if you need more detailed background information on the operation of StoneGate than what is offered in this chapter.

Supported Platforms

Sensors and analyzers can be run on the following general types of platforms:

- Purpose-built StoneGate IPS appliances.
- Standard Intel-compatible servers. Search for the version-specific *Hardware Requirements* in the technical documentation search at <http://www.stonesoft.com/en/support/>.
- As a VMware virtual host. There are some additional requirements and limitations when StoneGate IPS is run as a virtual host. See the Release Notes for more information. Detailed instructions can be found in [Installing and Activating StoneGate IPS in VMWare ESX Server](#) in the StoneGate Technical Documentation database.

The sensors and analyzers have an integrated, hardened Linux operating system that is always a part of the StoneGate engine software, eliminating the need for separate operating system installation, configuration, and patching.

Date and Time Settings

The time settings of the engines do not need to be adjusted, as they are automatically synchronized to the Management Server's time setting. For this operation, the time is converted to UTC time according to the Management Server's time zone setting.

Capture Interfaces

Sensors can be connected to a switch SPAN port or a network TAP to capture network traffic. Hubs can be used, but are not recommended. The considerations for these connection methods are explained below. Additionally, the IPS Sensor can be installed in-line, so that the network traffic is routed through the Sensor, allowing active blocking of any connection.

For more specific information on compatibility of different network devices and StoneGate IPS, refer to the Stonesoft website at <http://www.stonesoft.com/support/>.

Switch SPAN Ports

A *Switched Port Analyzer* (SPAN) port is used for capturing network traffic to a defined port on a switch. This is also known as *port mirroring*. The capturing is done passively, so it does not interfere with the traffic.

A Sensor's capture interface can be connected directly to a SPAN port of a switch. All the traffic to be monitored must be copied to this SPAN port.

Network TAPs

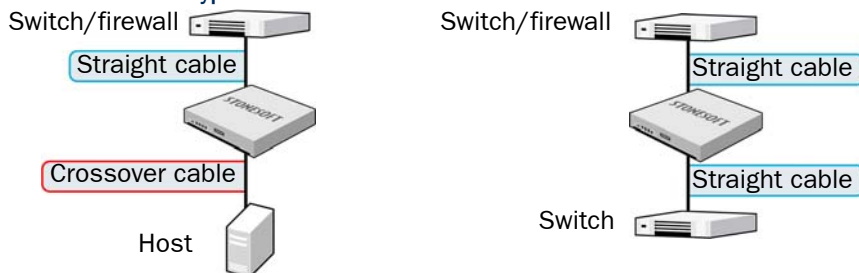
A *Test Access Port* (TAP) is a passive device located at the network wire between network devices. The capturing is done passively, so it does not interfere with the traffic. With a network TAP, the two directions of the network traffic is divided to separate wires. For this reason, the Sensor needs two Capture interfaces for a network TAP; one capture interface for each direction of the traffic. The two related Capture interfaces must have the same *Logical interface* that combines the traffic of these two interfaces for inspection. You could also use the pair of Capture interfaces to monitor traffic in two separate network devices.

Cabling Guidelines

Follow standard cabling with inline IPS: use straight cables to connect the sensor to switches/hubs and crossover cables to connect the sensor to hosts. Both crossover and straight cables may work when the sensors are operating normally due to software-level correction, but only the correct type of cable allows traffic to flow when fail-open network cards must pass traffic without the help of higher-level features.

Also, make sure the cables are correctly rated (CAT 5e or CAT 6 in gigabit networks).

Illustration 2.1 Correct Cable Types

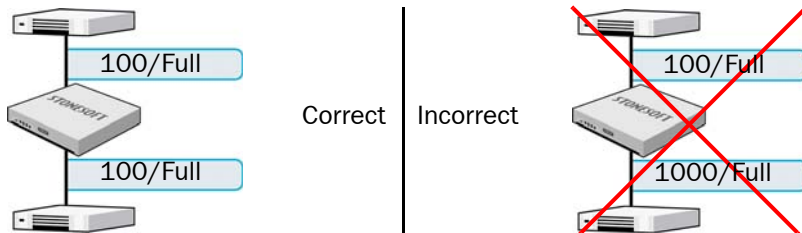


Speed And Duplex

Mismatched speed and duplex settings are a frequent source of networking problems. The basic principle for speed and duplex is simply that network cards at both ends of each cable must have identical settings. This principle also applies to the automatic negotiation setting: if one end of the cable is set to autonegotiate, the other end must also be set to autonegotiate and not to any fixed setting. Gigabit standards require interfaces to use autonegotiation—fixed settings are not allowed at gigabit speeds.

Inline interfaces of sensors require additional consideration: since the sensor is a “smart cable”, the settings must be matched on both links within each inline interface pair (identical settings on all four interfaces) instead of just matching settings at both ends of each cable (two + two interfaces). If one of the links has a lower maximum speed than the other link, the higher-speed link must be set to use the lower speed.

Illustration 2.2 Speed/Duplex Settings



CHAPTER 3

INSTALLING IPS LICENSES

This chapter instructs how to generate and install licenses for sensors and analyzers.

The following sections are included:

- ▶ [Getting Started with IPS Licenses](#) (page 20)
- ▶ [Generating New Licenses](#) (page 20)
- ▶ [Installing Licenses](#) (page 21)

Getting Started with IPS Licenses

Each analyzer and sensor engine must have its own license. You must generate the license files and install them on the Management Server using the Management Client before you can bring your system fully operational. The Management Server's license may also be limited to managing only a certain number of engines.

Your system may be able to automatically generate licenses for new StoneGate appliances. For automatic licensing to work, ensure that automatic updates are working in the Management Center. A factory-installed temporary license is automatically replaced with a permanent license bound to the serial code (POS) of the appliance after the appliance is configured for use.

If you do not need to install licenses for the IPS engines at this time, proceed to one of the following:

- If NAT is applied to communications between any system components, proceed to [Configuring NAT Addresses](#) (page 23).
- If NAT is not applied to the communications, you are ready to define the Sensor and Analyzer element(s). Proceed to [Defining Sensors and Analyzers](#) (page 31).

Configuration Overview

The following steps are needed for installing licenses for sensors and analyzers.

1. Generate the licenses at the Stonesoft website. See [Generating New Licenses](#) (page 20).
2. Install the licenses in the Management Client. See [Installing Licenses](#) (page 21).

Generating New Licenses

You generate the licenses at the Stonesoft website based on your *proof-of-license* (POL), included in the order confirmation message sent by Stonesoft or the proof-of-serial-number (POS) printed on the side of StoneGate appliances. Evaluation licenses are also available at the website. If you are licensing several components of the same type, remember to generate one license for each.

▼ To generate a new license

1. Browse to the Stonesoft License Center at my.stonesoft.com/managelicense.do.
2. Enter the POL code in the **License Identification** field and click **Submit**. The license page opens.
3. Click **Register**. The license generation page opens.
4. Enter the Management Server's proof-of-license code or the engine's primary control IP address for the engines you want to license.
 - The Management Server's proof-of-license can be found in the e-mail you received detailing your licenses or in the Management Client for all licenses imported into the system.
5. Click **Submit Request**. The license file is sent to you in a moment. It also becomes available for download at the license page.

Note – Evaluation license requests may need manual processing. See the license page for current delivery times and details.



Installing Licenses

To install licenses, the license files must be available to the computer you use to run the Management Client.



Note - All licenses can be installed even though you have not yet defined all the elements the licenses will be bound to.

▼ To install StoneGate licenses

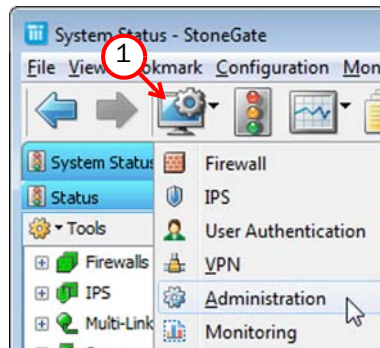
1. Select **File**→**System Tools**→**Install Licenses**.



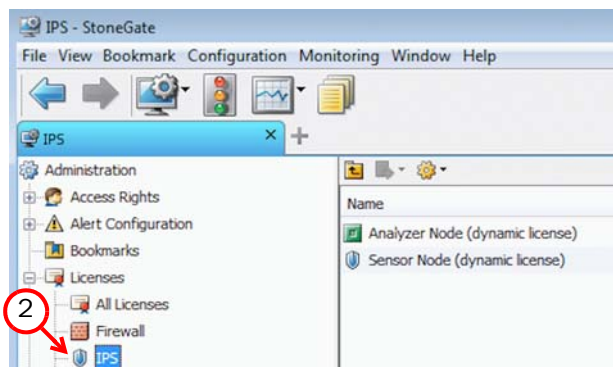
2. Select one or more license files in the dialog that opens.

▼ To check that the licenses were installed correctly

1. Click the Configuration icon in the toolbar and select **Administration**. The Administration Configuration view opens.



2. Expand the **Licenses** branch and select **IPS**.



You should see one license for each analyzer and sensor engine. If you have Management-bound engine licenses, you must bind them manually to the correct engines once you have configured the engine elements.

What's Next?

- ▶ If NAT is applied to communications between system components, proceed to [Configuring NAT Addresses](#) (page 23).
- ▶ Otherwise, you are ready to define the Sensor and Analyzer element(s). Proceed to [Defining Sensors and Analyzers](#) (page 31).

CHAPTER 4

CONFIGURING NAT ADDRESSES

This chapter contains the steps needed to configure Locations and contact addresses when a NAT (network address translation) operation is applied to the communications between the sensor or analyzer and other StoneGate components.

The following sections are included:

- ▶ [Getting Started with NAT Addresses](#) (page 24)
- ▶ [Defining Locations](#) (page 25)
- ▶ [Adding SMC Server Contact Addresses](#) (page 26)

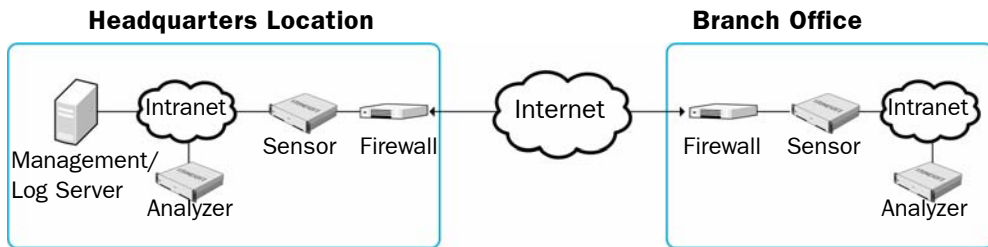
Getting Started with NAT Addresses

If there is *network address translation* (NAT) between communicating system components, the translated IP address may have to be defined for system communications. All communications between the StoneGate components are presented as a table in [Default Communication Ports](#) (page 95).

You use *Location* elements to configure StoneGate components for NAT. There is a Default Location to which all elements belong if you do not assign them a specific Location. If NAT is applied between two system components, you must separate them into different Locations and then add a contact address for the component that needs to be contacted.

You can define a Default contact address for contacting a component (defined in the Properties dialog of the corresponding element). The component's Default contact address is used in communications when components that belong to another Location contact the component and the component has no contact address defined for their Location.

Illustration 4.1 An Example Scenario for Using Locations



In the example scenario above, a Management Server and a Log Server manage StoneGate components both at a company's headquarters and in a branch office.

NAT could typically be applied at the following points:

- The firewall at the headquarters or an external router may provide the SMC servers external IP addresses on the Internet. The external addresses must be defined as contact addresses so that the components at the branch offices can contact the servers across the Internet.
- The branch office firewall or an external router may provide external addresses for the StoneGate components at the branch office. Also in this case, the external IP addresses must be defined as contact addresses so that the Management Server can contact the components.

When contact addresses are needed, it may be enough to define a single new Location element, for example, for the branch office, and to group the StoneGate components at the branch office into the "Branch Office" Location. The same Location element could also be used to group together StoneGate components at any other branch office when they connect to the SMC servers at the headquarters.

Configuration Overview

To add contact addresses, proceed as follows:

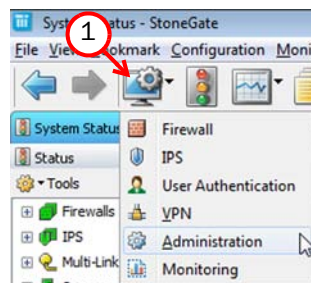
1. Define Location element(s). See [Defining Locations](#) (page 25).
2. Define contact addresses for the Management Server and Log Server(s). See [Adding SMC Server Contact Addresses](#) (page 26).
3. Select the correct Location for the IPS engines when you create the Sensor and Analyzer elements. See [Defining Sensors and Analyzers](#) (page 31).

Defining Locations

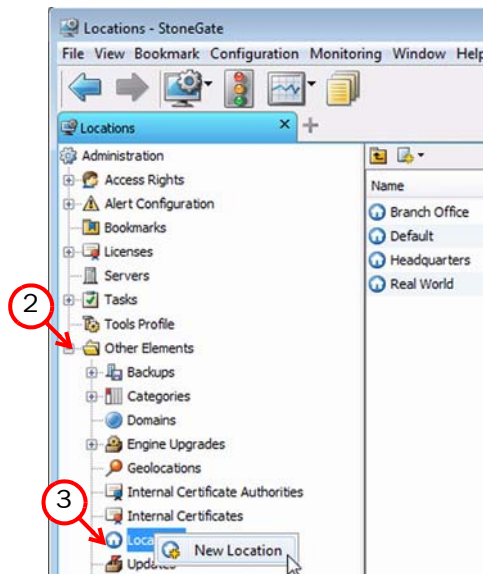
The first task is to group the system components into Location elements based on which components are on the same side of a NAT device. The elements that belong to the same Location element always use the primary IP address (defined in the main Properties dialog of the element) when contacting each other.

▼ To create a new Location element

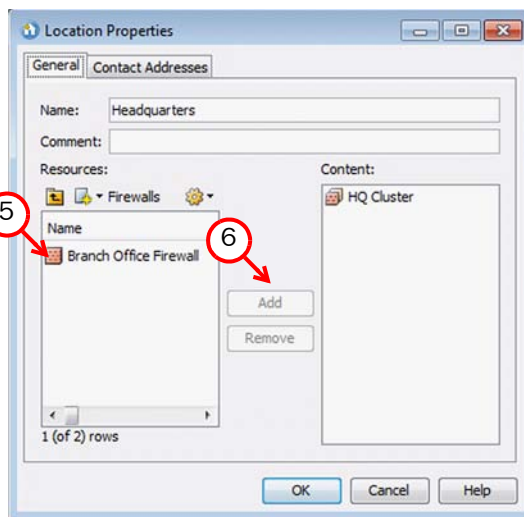
1. Click the Configuration icon in the toolbar, and select **Administration**. The Administration Configuration view opens.



2. Expand **Other Elements** in the tree view.



3. Right-click **Locations** and select **New Location**. The Location Properties dialog opens.



4. Type in a **Name**.

5. Select element(s).

6. Click **Add**.

7. Repeat steps 5-6 until all necessary elements are added.

8. Click **OK**.

Repeat to add other Locations as necessary.

What's Next?

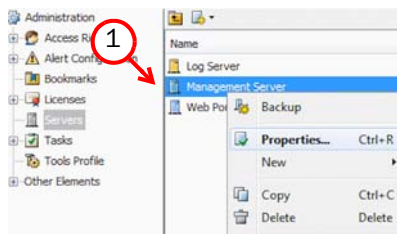
- ▶ If your Management Server or Log Server needs a contact address configuration, proceed to [Adding SMC Server Contact Addresses](#) (page 26).
- ▶ If you plan to add contact addresses only for Sensor or Analyzer elements, proceed to [Defining Sensors and Analyzers](#) (page 31).

Adding SMC Server Contact Addresses

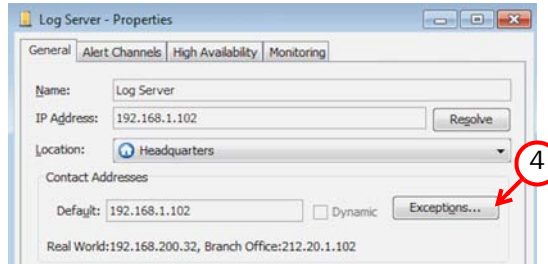
The Management Server and the Log Server can have more than one contact address for each Location. This allows you, for example, to define a contact address for each Internet link in a Multi-Link configuration for remotely managed components.

▼ To define the Management Server and Log Server contact addresses

1. Right-click a server and select **Properties**. The Properties dialog for that server opens.



2. Select the **Location** of this server.
3. Enter the **Default** contact address. If the server has multiple alternative IP addresses, separate the addresses with commas.



4. Click **Exceptions** and define Location-specific contact addresses if the Default Contact Address(es) are not valid from all other Locations.



Note – Elements grouped in the same Location element always use the primary IP address (defined in the main Properties dialog of the element) when contacting each other. All elements not specifically put in a certain Location are treated as if they belonged to the same Location.

Close the server properties and define the contact addresses for other servers in the same way.

What's Next?

- ▶ [Defining Sensors and Analyzers](#) (page 31).

CONFIGURING SENSORS AND ANALYZERS

In this section:

Defining Sensors and Analyzers - 31

Saving the Initial Configuration - 45

Configuring Routing and Installing Policies - 51

CHAPTER 5

DEFINING SENSORS AND ANALYZERS

This chapter contains the steps needed to complete the sensor and analyzer configuration that prepares the Management Center for a StoneGate sensor and analyzer installation.

Very little configuration is done directly on the engines. Most of the configuration is done using the Management Client, so the engines cannot be successfully installed before defining them in the Management Center as outlined in this chapter.

The following sections are included:

- ▶ [Getting Started with Defining Sensors and Analyzers](#) (page 32)
- ▶ [Creating Engine Elements](#) (page 32)
- ▶ [Defining System Communication Interfaces for IPS Engines](#) (page 33)
- ▶ [Setting Interface Options for IPS Engines](#) (page 37)
- ▶ [Defining Traffic Inspection Interfaces for Sensors](#) (page 38)
- ▶ [Bypassing Traffic on Overload](#) (page 43)
- ▶ [Finishing the Engine Configuration](#) (page 44)

Getting Started with Defining Sensors and Analyzers

The Sensor and Analyzer elements are a tool for configuring nearly all aspects of your physical IPS components.

An important part of the Sensor and Analyzer elements are the interface definitions. There are two main categories of Sensor and Analyzer interfaces:

- Interfaces for system communications. They are used when the Sensor or the Analyzer is the source or the final destination of the communications (for example, in control communications between the Sensor or Analyzer and the Management Server). You must define at least one interface that is dedicated to system communications for each Sensor and Analyzer element.
- Interfaces for inspecting traffic. You must define one or more traffic inspection interfaces for each Sensor element.

The interfaces have their own numbering in the Management Center called Interface ID. The numbering is independent of the operating system interface numbering on the engines. However, if you do the engine's initial configuring using the automatic USB memory stick configuration method, the Interface IDs in the Management Center are mapped to match the physical interface numbering in the operating system (eth0 is mapped to Interface ID 0 and so on). If you do the initial configuration manually, you can freely choose how the Interface IDs in the Management Center are mapped to the physical interfaces.

Creating Engine Elements

There are two main installation types. The Sensor and the Analyzer can be installed as a combined Sensor-Analyzer on the same machine, or as separate Sensor and Analyzer engines on separate machines. A combined Sensor-Analyzer is both a Sensor and an Analyzer, and has the properties of both element types in the configuration tools.

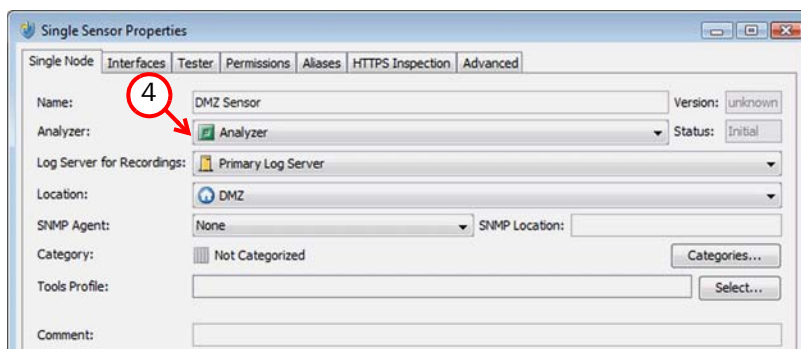
This section covers the basic configuration of a Sensor and Analyzer elements. For complete instructions on configuring Sensor and Analyzer properties, see the *Online Help* of the Management Client or the *Administrator's Guide* PDF.

▼ To create an engine element

1. Click the Configuration icon in the toolbar and select **IPS**. The IPS Configuration view opens.



2. Right-click **IPS Engines** and select one of the following:
 - **New**→**Analyzer**
 - **New**→**Combined Sensor-Analyzer**
 - **New**→**Sensor Cluster**
 - **New**→**Single Sensor**.
3. Enter a unique **Name**.



4. (*Sensors only*) Select the **Analyzer** to which the Sensor sends event data.
5. Select the Log Server options according to the type of element you are creating:

Element Type	Option	Description
Analyzer	Log Server	Select the Log Server to which the Analyzer sends event logs.
Analyzer	Log Server for Alerts	(Optional) Select the Log Server to which the Analyzer sends alerts. If no Log Server is selected, alerts are sent to the same Log Server as event logs.
Sensor	Log Server for Recordings	(Optional) Select the Log Server to which the Sensor sends traffic recordings. If no Log Server is selected, the Sensor does not make any traffic recordings.

6. If required in your setup, select the **Location** (see [Configuring NAT Addresses](#) (page 23)).

Defining System Communication Interfaces for IPS Engines

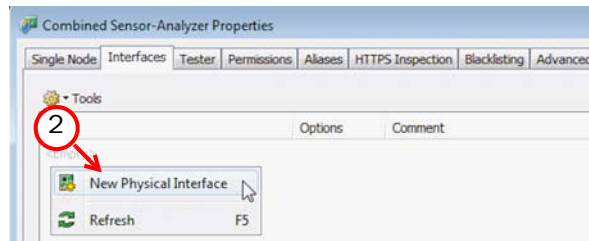
Each IPS engine needs at least one interface for communicating with other system components. More than one system communication interface can be added to provide a primary and a backup interface for Management Server communications.

For Analyzers, the volume of log traffic can easily grow large enough to delay other connections. You may want to have dedicated interface(s) for receiving event data from sensors.

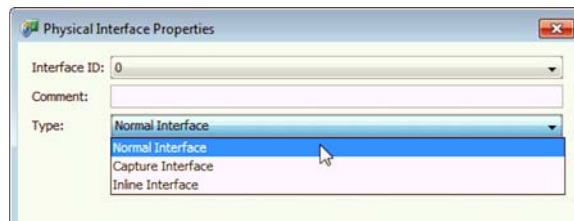
Defining Physical Interfaces

▼ To define a physical interface

1. Switch to the **Interfaces** tab.



2. Right-click and select **New Physical Interface**. The Physical Interface Properties dialog opens.



3. Select the **Interface ID**.
4. (Not applicable to Analyzers) Select **Normal Interface** as the **Type**.
5. Click **OK**.

The physical interface is added to the interface list. Add the necessary number of interfaces in the same way.

What's Next?

- ▶ If you want to add VLANs to the physical interface, continue by [Defining VLAN Interfaces](#) (page 35).
- ▶ Otherwise, continue by [Defining IP Addresses](#) (page 36).

Defining VLAN Interfaces

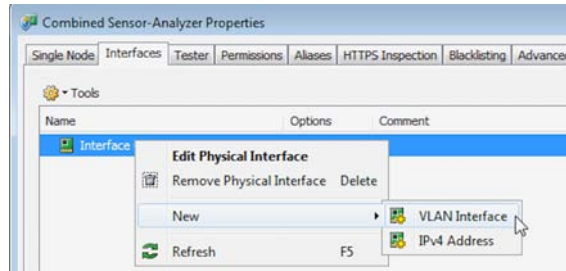
VLANs divide a single physical network link into several virtual links. You can add up to 4094 VLANs per interface. Analyzers cannot use VLANs.



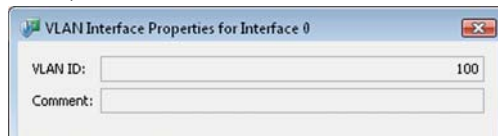
Caution – Do not add any manual VLAN definitions to an interface you want to use for sending resets. Adding VLANs prevents selecting the interface as a reset interface and also removes the reset interface from any existing selections.

▼ To define a VLAN Interface

1. Right-click a physical interface and select **New**→**VLAN Interface**. The Interface Properties dialog opens.



2. Enter the **VLAN ID** (1-4094).



Note – The VLAN ID must be the same VLAN ID used in the switch at the other end of the VLAN trunk.

3. Click **OK**.

The specified VLAN ID is added to the physical interface.

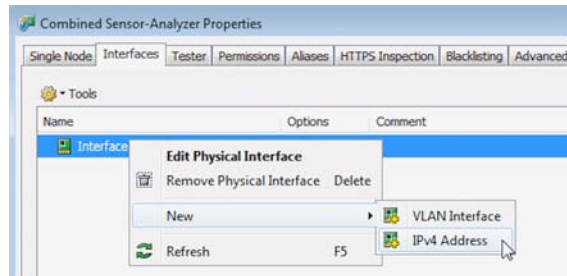
Repeat the steps above to add further VLANs to the interface.

The VLAN interface is now ready to be used as a network interface. The VLAN interface is identified as *Interface-ID.VLAN-ID*, for example 2.100 for Interface ID 2 and VLAN ID 100.

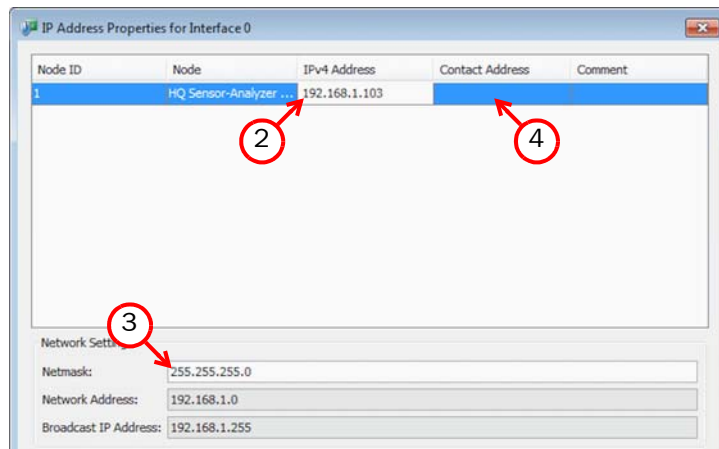
Defining IP Addresses

▼ To define an IP address

1. Right-click a physical interface or a VLAN interface and select **New→IP Address**. The IP Address Properties dialog opens.



2. Double-click the **IPv4 Address** cell and enter the IPv4 Address. Repeat for each node if this is a Sensor Cluster element.
3. Enter the **Netmask**.

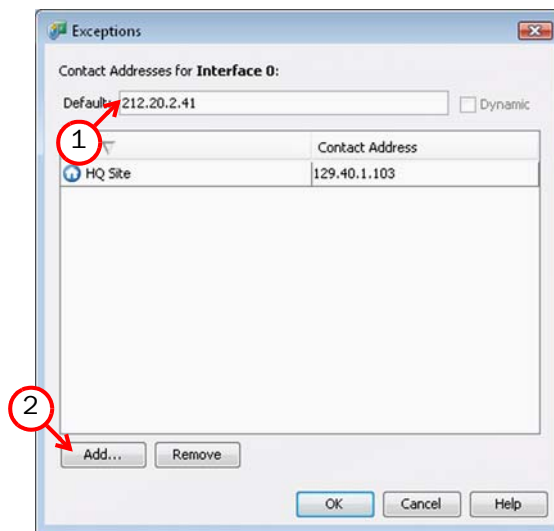


4. If NAT is applied to system communications, double-click the **Contact Address** cell and continue as explained in the next illustration. Otherwise, Click **OK** to close the IP Address Properties dialog.

▼ To define a contact address

1. Enter the **Default** contact address to define the translated IP address of this engine. It is used by default by components in a different Location.

2. (Optional) Click **Add** to define a different contact address for contacting this engine from some specific Location.



3. Click **OK** to close the Contact Addresses dialog.
4. Click **OK** to close the IP Address Properties dialog.

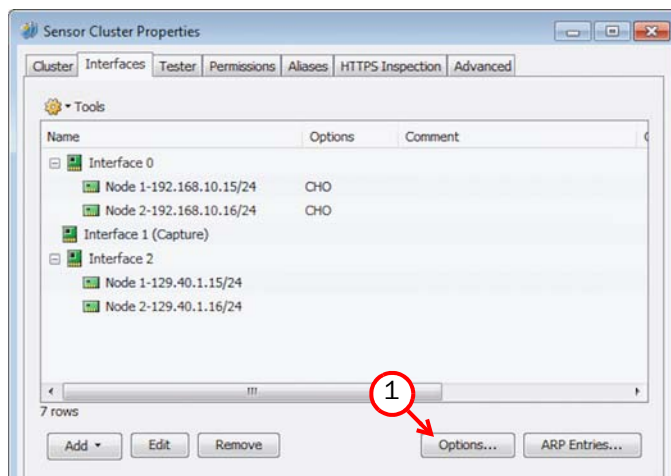
You can define several IP addresses for the same physical network interface. Before you continue, write down the networks to which each Interface ID is connected.

Setting Interface Options for IPS Engines

Interface options allow you to select which interfaces are used for which types of system communications.

▼ To set the Interface Options

1. Click **Options**. The Interface Options dialog opens.



2. Select the **Primary** Control Interface for communications with the Management Server.

3. (Optional) Select a **Backup** Control interface that is used if the Primary interface is not available.
4. (Sensor Cluster only) Select the **Primary** Heartbeat Interface for communications between the nodes of the cluster. This must not be a VLAN interface.



Caution – Heartbeat traffic is time-critical. A dedicated network (without other traffic) is strongly recommended for security and reliability of heartbeat communication.

5. (Sensor Cluster only, recommended) Select a second Physical Interface as the **Backup** Heartbeat interface.
6. Select the **Log/Analyzer communication source IP address**.
 - On Sensors, this is for relaying information about the processed traffic to the Analyzer for further processing.
 - On Analyzers and Sensor-Analyzers, this is for relaying logs and alerts to the Log Server.
7. Click **OK**.

Defining Traffic Inspection Interfaces for Sensors

Sensors are the IPS components that inspect traffic. The traffic can either be captured for inspection through the sensor's capture interfaces, or it can be inspected as it flows through the sensor's inline interfaces. You can define both capture interfaces and inline interfaces for the same sensor.

A sensor can actively filter only traffic that attempts to pass through its inline interfaces. However, it can reset traffic picked up through capture interfaces if you set up specific reset interfaces. The reset interfaces can send TCP resets and ICMP "destination unreachable" messages when the communications trigger a response. You can use a system communications interface for sending resets if the resets are routed correctly through that interface and there are no VLANs on the interface.

When traffic is inspected, it may be important to know the interface through which it arrives to the sensor. It is also important to be able to distinguish a sensor's capture interfaces from its inline interfaces. Logical Interface elements are used for both these purposes. They allow you to group together interfaces that belong to the same network segment and to identify the type of the traffic inspection interface (capture interface or inline interface).

What's Next?

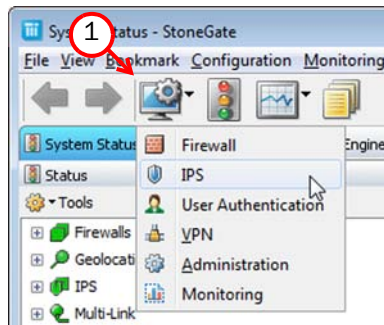
- ▶ If you want to create both capture and inline interfaces on the same sensor, or if you want to create logical interfaces to distinguish interfaces from each other, proceed to [Defining Logical Interfaces](#) (page 39).
- ▶ If you do not want to use an existing system communication interface as the reset interface, define the new reset interfaces as instructed in [Defining Reset Interfaces](#) (page 40).
- ▶ To define capture interfaces, proceed to [Defining Capture Interfaces](#) (page 41).
- ▶ To define inline interfaces, proceed to [Defining Inline Interfaces](#) (page 42).

Defining Logical Interfaces

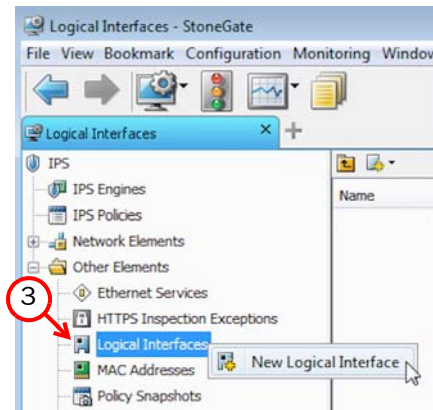
A Logical Interface is used in the IPS policies and the traffic inspection process to represent a network segment. The StoneGate system contains one default Logical Interface. A Logical interface can represent any number or combination of interfaces and VLAN interfaces, except that the same Logical interface cannot be used to represent both capture interfaces and inline interfaces on the same Sensor. The rules in the ready-made IPS Strict Template and IPS System Template match all Logical Interfaces.

▼ To define a Logical interface

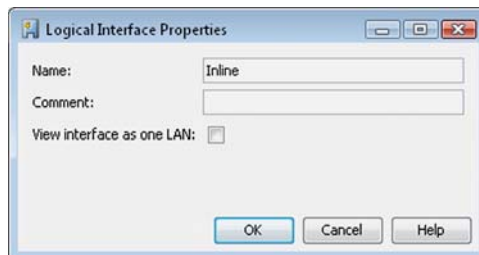
1. Click the Configuration icon in the toolbar and select **IPS**. The IPS Configuration view opens.



2. Expand the **Other Elements** branch.



3. Right-click **Logical Interfaces** and select **New Logical Interface**. The Logical Interface Properties dialog opens.



4. Enter a unique **Name**.

5. (Optional) If you use VLAN tagging on capture or inline interfaces, select **View interface as one LAN** if you do not want the sensor to see a single connection as multiple connections when a switch passes traffic between different VLANs and all traffic is mirrored to the sensor through a SPAN port.
6. Click **OK**.

Repeat these steps to define any additional Logical Interfaces.

What's Next?

- ▶ If you want to use reset interfaces together with capture interfaces, define the reset interfaces first. Proceed to [Defining Reset Interfaces](#) (page 40).
- ▶ To define capture interfaces, proceed to [Defining Capture Interfaces](#) (page 41).
- ▶ To define inline interfaces, proceed to [Defining Inline Interfaces](#) (page 42).

Defining Reset Interfaces

Reset interfaces can deliver TCP resets and ICMP “destination unreachable” messages to interrupt communications picked up from capture interfaces when the communications trigger a response.

VLANs are supported for sending resets, but the correct VLAN is selected automatically. An interface you want to use as the reset interface must not have any manually added VLAN configuration.

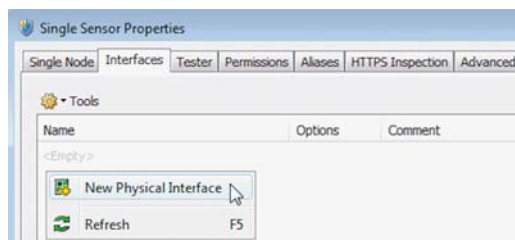
The reset interface must be in the same broadcast domain as the capture interface that uses the reset interface. The resets are sent using the IP addresses and MAC addresses of the communicating hosts.



Note – An interface that is used *only* as a reset interface must not have an IP address.

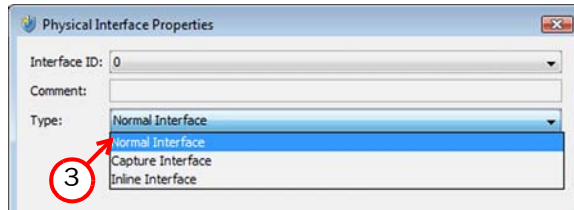
▼ To define a reset interface

1. Right-click and select **New Physical Interface**. The Physical Interface Properties dialog opens.



2. Select the **Interface ID**.

3. Select **Normal Interface** as the **Type**.



4. Click **OK**.

This interface can now be used as a reset interface. When you set up the physical network, make sure that the reset interface connects to the same network as the capture interface(s).

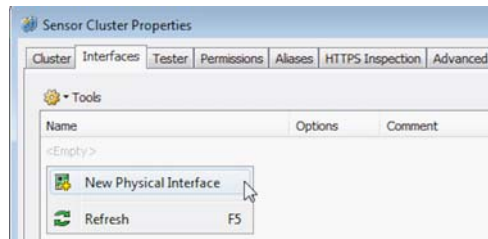
Defining Capture Interfaces

Capture interfaces listen to traffic that is not routed through the Sensor. You can have as many capture interfaces as there are available physical ports on the sensor (there are no license restrictions regarding this interface type).

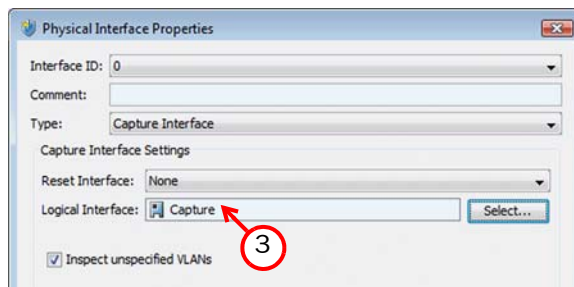
External equipment must be set up to mirror traffic to the capture interface. You can connect a capture interface to a switch SPAN port or a network TAP to capture traffic. For more information, see [Capture Interfaces](#) (page 16).

▼ To define a capture interface

1. Right-click and select **New Physical Interface**. The Physical Interface Properties dialog opens.



2. Select the **Interface ID**.
3. Select **Capture Interface** as the **Type**.



4. (Optional) Select a TCP **Reset Interface** for traffic picked up through this capture interface.
5. If your configuration requires you to change the **Logical Interface**, click **Select** and select the Logical interface in the dialog that opens.

6. Click **OK**.

Repeat these steps to define any additional capture interfaces.

What's Next?

- ▶ To define inline interfaces, proceed to [Defining Inline Interfaces](#) (page 42).
- ▶ To define how an inline sensor handles traffic when the traffic load is too high, proceed to [Bypassing Traffic on Overload](#) (page 43).
- ▶ Otherwise, proceed to [Finishing the Engine Configuration](#) (page 44).

Defining Inline Interfaces

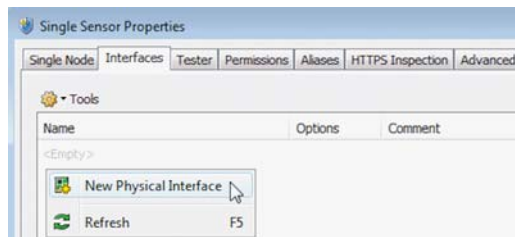
The number of inline interfaces you can have are limited by the license in use. One inline interface always comprises two physical interfaces, as the traffic is forwarded from one interface to the other. The allowed traffic passes through as if it was going through a network cable. The traffic you want to stop is dropped by the Sensor.

Inline interfaces (like capture interfaces) are associated with a Logical Interface, which is used in the IPS policies and the traffic inspection process to represent one or more Sensor interfaces.

Fail-open network cards have fixed pairs of ports. Take particular care to map these ports correctly during the initial configuration of the engine. Otherwise, the network cards do not correctly fail open when the sensor is offline. If you use the automatic USB memory stick configuration method for the engine's initial configuration, the ports are configured automatically. See [Configuring the Engine Automatically with a USB Stick](#) (page 64) for more information.

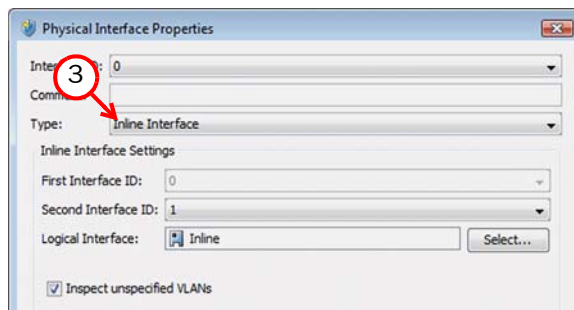
▼ To define an inline interface

1. Right-click and select **New Physical Interface**. The Physical Interface Properties dialog opens.



2. Select the **Interface ID**.

3. Select **Inline Interface** as the **Type**.



4. (Optional) Change the automatically selected **Second Interface ID**.
5. Leave **Inspect Unspecified VLANs** selected if you want the sensor to inspect traffic also from VLANs that are not included in the sensor's interface configuration.
6. If your configuration requires you to change the **Logical Interface** from Default_Eth, click **Select** and select the Logical interface in the dialog that opens.
7. Click **OK**.

Repeat these steps to define any additional inline interfaces.

What's Next?

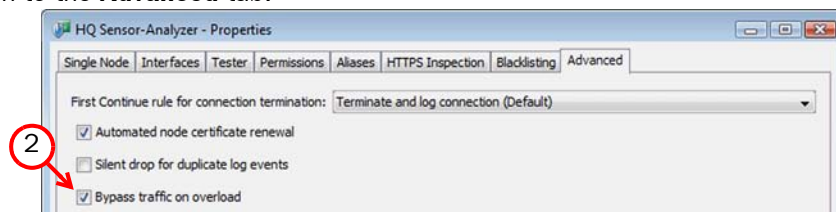
- ▶ To define how an inline sensor handles traffic when the load is too high, proceed to [Bypassing Traffic on Overload](#) (page 43).
- ▶ Otherwise, proceed to [Finishing the Engine Configuration](#) (page 44).

Bypassing Traffic on Overload

By default, inline sensors inspect all connections. If the traffic load is too high for the inline sensor to inspect all the connections, some traffic may be dropped. Alternatively, inline sensors can dynamically reduce the number of inspected connections if the load is too high. This can improve performance in evaluation environments, but some traffic may pass through without any access control or inspection.

▼ To bypass traffic on overload

1. Switch to the **Advanced** tab.



2. Select **Bypass traffic on overload**.

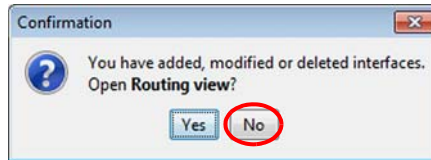
What's Next?

- ▶ Proceed to [Finishing the Engine Configuration](#) (page 44).

Finishing the Engine Configuration

▼ To finish the engine configuration

1. Write down the networks to which each Interface ID is connected
2. Click **OK** close the engine properties. The following notification opens.



3. Click **No**.

What's Next?

- ▶ You are now ready to transfer the configuration to the physical Sensor and Analyzer engines. Proceed to [Saving the Initial Configuration](#) (page 45).

CHAPTER 6

SAVING THE INITIAL CONFIGURATION

This chapter explains how to save the Sensor and Analyzer initial configuration in the Management Center and how to transfer it to the physical sensor and analyzer engines.

The following sections are included:

- ▶ [Configuration Overview](#) (page 46)
- ▶ [Saving the Initial Configuration for Sensors and Analyzers](#) (page 46)
- ▶ [Transferring the Initial Configuration to Sensors and Analyzers](#) (page 49)

Configuration Overview

Once you have configured the Sensor and Analyzer elements in the Management Client, you must transfer the initial configuration to the physical sensor and analyzer engines.

You must complete the following steps:

1. Save the initial configuration in the Management Client. See [Saving the Initial Configuration for Sensors and Analyzers](#) (page 46).
2. Transfer the initial configuration to the physical sensor and analyzer engines. See [Transferring the Initial Configuration to Sensors and Analyzers](#) (page 49).

Saving the Initial Configuration for Sensors and Analyzers

The initial configuration sets some basic parameters for the Sensors and Analyzers and triggers the creation of one-time passwords needed to establish a connection with the Management Server.

There are three ways to initialize your IPS engines and establish contact between them and the Management Server.

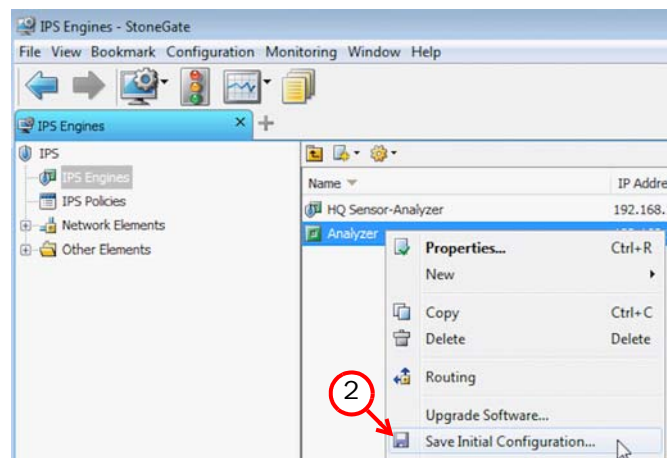
- You can write down the one-time password and enter all information manually in the command-line Configuration Wizard on the engines.
- You can save the configuration on a floppy disk or a USB memory stick and make some manual changes in the command-line Configuration Wizard on the engines.
- You can save the initial configuration on a USB memory stick and use the memory stick to automatically configure the engine without using the Configuration Wizard.



Note – The automatic configuration is primarily intended to be used with StoneGate appliances, and may not work in all other environments.

▼ To save the initial configuration

1. Select **IPS Engines**. A list of IPS engine elements opens.



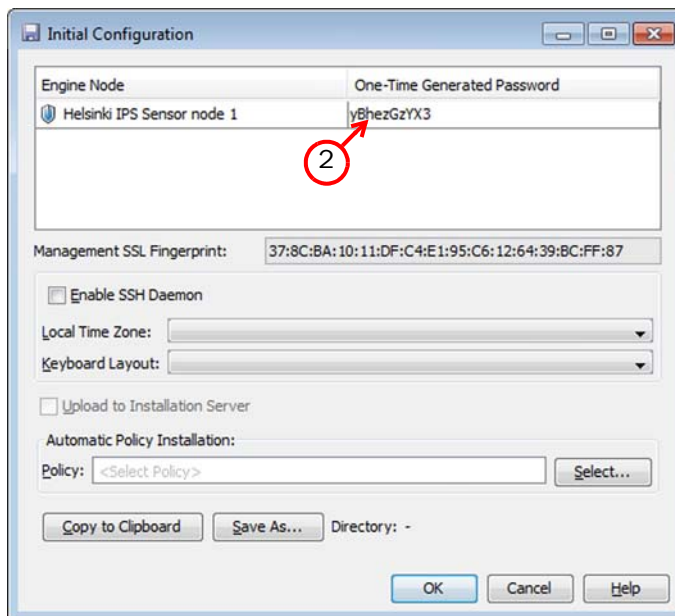
2. Right-click the Sensor or Analyzer element and select **Save Initial Configuration**. The Initial Configuration dialog opens.

What's Next?

- ▶ If you want to use the Configuration Wizard, proceed to the section [To prepare for configuration using the Configuration Wizard](#) (page 47).
- ▶ For fully automatic configuration, proceed to the section [To prepare for fully automatic configuration](#) (page 48).

▼ To prepare for configuration using the Configuration Wizard

1. (Optional) If you plan to enter the information manually, write down or copy the **Management SSL Fingerprint**. Using the fingerprint increases the security of the communications when the engine contacts the Management Server.



2. If you plan to enter the information manually, write down or copy the **One-Time Generated Password** for each engine. Keep track of which password belongs to which node.
3. (Optional) If you plan to import the configuration in the Configuration Wizard, you can **Enable SSH Daemon** and select the **Local Time Zone** and **Keyboard Layout**.
4. (Sensors only) Click **Select** and select the appropriate policy if you already have a policy you want to use. The selected policy is automatically installed after the Sensor has contacted the Management Server. See [Installing the Initial Policy](#) (page 55) for descriptions of the available pre-defined policies.
5. If you plan to import the configuration in the Configuration Wizard, click **Save As** and save the configuration on a USB memory stick.
6. Click **Close**.

What's Next?

- ▶ Proceed to [Transferring the Initial Configuration to Sensors and Analyzers](#) (page 49).

▼ To prepare for fully automatic configuration

1. (Optional) **Enable SSH Daemon** to allow remote access to the engine command line.
2. Select the **Local Time Zone** and **Keyboard Layout** for the engine.

The screenshot shows the 'Initial Configuration' window. At the top, there are two columns: 'Engine Node' with the value 'Helsinki IPS Sensor node 1' and 'One-Time Generated Password' with the value 'yBhezGzYX3'. Below this is a table with the same data. Underneath, there is a 'Management SSL Fingerprint' field with the value '37:8C:BA:10:11:DF:C4:E1:95:C6:12:64:39:BC:FF:87'. A red circle with the number 1 points to the 'Enable SSH Daemon' checkbox, which is checked. Below that, 'Local Time Zone' is set to 'Europe/Helsinki' and 'Keyboard Layout' is set to 'Finnish'. There is an unchecked checkbox for 'Upload to Installation Server'. Under 'Automatic Policy Installation', there is a 'Policy:' dropdown menu showing 'System Policy' and a 'Select...' button. A red circle with the number 3 points to the 'Select...' button. Below the policy selection, there is a 'Save As...' button and a 'Directory: -' field. A red circle with the number 4 points to the 'Save As...' button. At the bottom of the window are 'Copy to Clipboard', 'Save As...', 'Directory: -', 'OK', 'Cancel', and 'Help' buttons.

3. (Sensors only) Click **Select** and select the appropriate policy if you already have a policy you want to use. The selected policy is automatically installed after the Sensor has contacted the Management Server. See [Installing the Initial Policy](#) (page 55) for descriptions of the available pre-defined policies.
4. Click **Save As** and save the configuration on the root of a USB memory stick, so that the engine can boot from it.
5. Click **Close**.

Once the sensor or analyzer is fully configured, the SSH daemon can be set on and off using the Management Client. Enabling SSH in the initial configuration gives you remote command line access in case the configuration is imported correctly, but the engine fails to establish contact with the Management Server.

The time zone selection is used only for converting the UTC time that the engines use internally for display on the command line. All internal operations use UTC time, which is synchronized with the Management Server time once the engine is configured.

If you lose the one-time password or the saved configuration, you can repeat the procedure for the sensor or analyzer engines.



Caution – Handle the configuration files securely. They include the one-time password that allows establishing trust with your Management Server.

Transferring the Initial Configuration to Sensors and Analyzers

You are now ready to install the StoneGate sensor and analyzer engine(s). The initial configuration is transferred to the engines during the installation.

What's Next?

- ▶ If you have a StoneGate appliance, see the installation and initial configuration instructions in the *Appliance Installation Guide* that was delivered with the appliance. After this, return to this guide to set up basic routing and policies (see [Configuring Routing and Installing Policies](#) (page 51) or see the more detailed instructions in the *Online Help* of the Management Client or the *Administrator's Guide* PDF).
- ▶ If you are using another type of device as the sensor or analyzer engine, proceed to [Installing the Engine on Intel-Compatible Platforms](#) (page 61).

CHAPTER 7

CONFIGURING ROUTING AND INSTALLING POLICIES

After successfully installing the Sensor and Analyzer engines and establishing contact between the engine(s) and the Management Server, the engines are left in the initial configuration state. Now you must define basic routing and policies to be able to use the engines to inspect traffic. Both of these tasks are done using the Management Client.

The following sections are included:

- ▶ [Configuring Routing](#) (page 52)
- ▶ [Installing the Initial Policy](#) (page 55)

Configuring Routing

In StoneGate, routing is done entirely through the Management Client. The routing information of sensors and analyzers is only used for system communications. The inspected traffic is not routed. The sensor's Inline interfaces are always fixed as port pairs; traffic that enters through one port is automatically forwarded to the other port.

Most often only one or two simple tasks are needed to define routing information for Sensor and Analyzer elements:

- Define the default route. This is the route packets to any IP addresses not specifically included in the routing configuration should take.
- Add routes to your internal networks that are not directly connected to the Sensor or Analyzer if the networks cannot be reached through the default gateway.

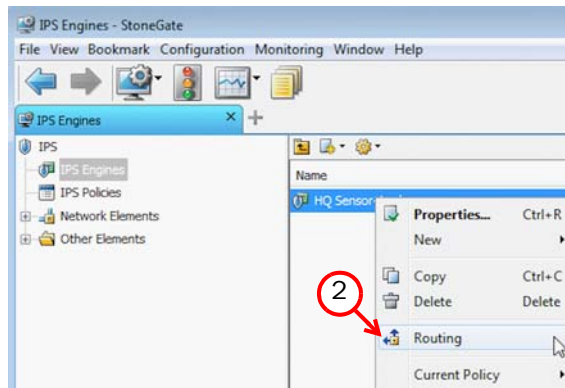
Routing is most often done using the following elements:

- **Network** elements: represent a group of IP addresses.
- **Router** elements: represent the gateway devices that will forward packets to the networks you add in the routing configuration.

When you modify interfaces and then close the Analyzer or Sensor properties, you always receive a notification that allows you to open the Routing view directly. You can view the Routing view at any other time by selecting **Configuration**→**Routing** from the menu.

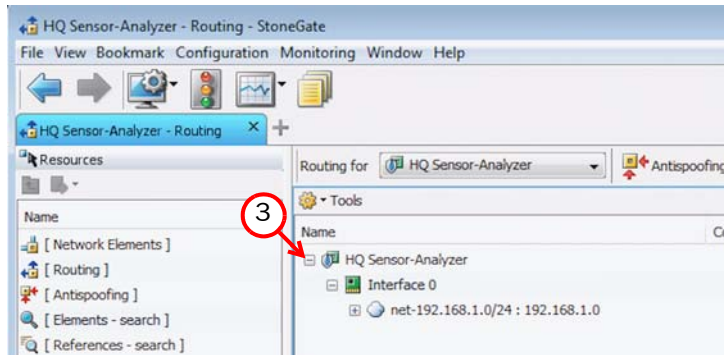
▼ To view routing information

1. Right-click the IPS element whose routing you want to configure.



2. Select **Routing**. The Routing view for the selected element opens.

All the Sensor or Analyzer element's physical interfaces and their network definitions have been automatically added to the Routing view. You can select another element to view its routing information.



- Expand the routing tree to view all the routing information for the interfaces.



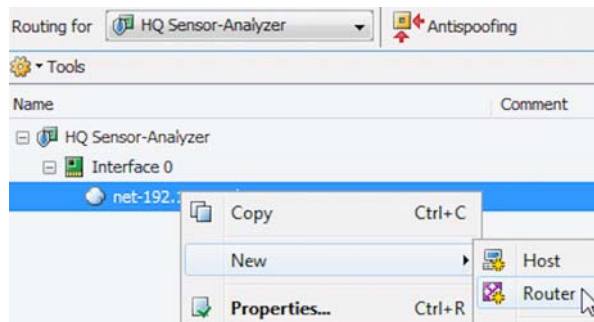
Note – Networks are only added automatically. Networks and interfaces are never deleted automatically. Inappropriate elements are marked with a symbol to show that they are invalid. You must delete the invalid elements manually if you do not want them to be shown in the Routing view.

Adding Next-hop Routers

For StoneGate IPS, you may need to define a default route in case the Management Center (Management Servers and Log Servers) and other system components are not located on a directly connected network. Other routes may be needed in addition to the default route if one or more system components are not directly connected and cannot be reached through the default gateway. To add the default route or to add other routes, you must first add a Router element to represent the gateway devices that forward packets to the networks.

▼ To add a router

- Right-click the Network and select **New**→**Router**. The Router Properties dialog opens.



- Fill in the name and IP address for the Router.

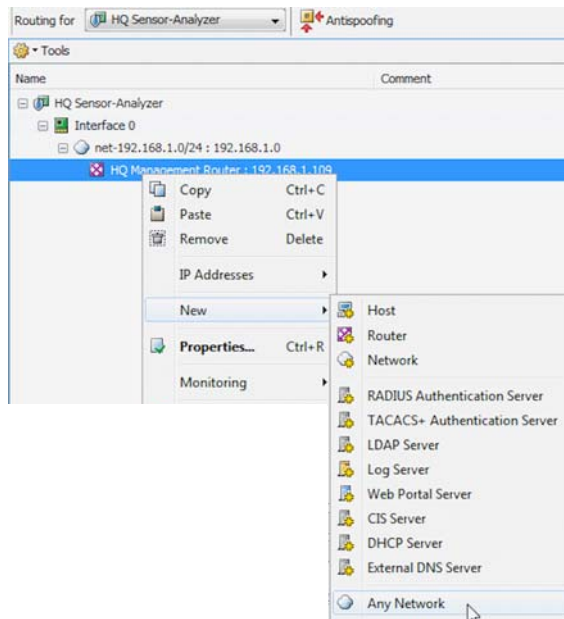
What's Next?

- ▶ If you want to define the default route, continue by [Adding the Default Route](#) (page 54).
- ▶ If you want to add other routes, continue by [Adding Other Routes](#) (page 54).

Adding the Default Route

▼ To add the default route

- ➔ Right-click the Router and select **New**→**Any Network**.



You are not actually creating a new element, just inserting the existing default element “Any Network”.

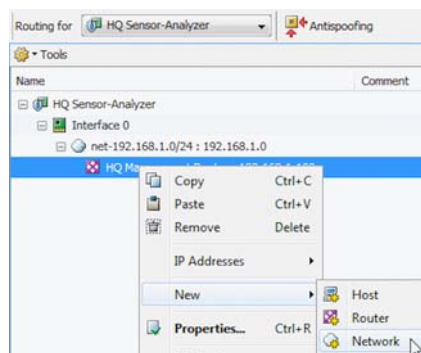
What's Next?

- ▶ To add other routes, proceed to [Adding Other Routes](#).
- ▶ Otherwise, proceed to [Installing the Initial Policy](#) (page 55).

Adding Other Routes

▼ To add other routes

1. Right-click the Router and select **New**→**Network**. The Network Properties dialog opens.



2. Give the network a unique a **Name** and enter the network space.

Repeat these steps to add any additional Networks to the Router element.

The routing configuration changes are transferred to the engine with the other configuration information when you install an IPS policy on the Sensor.

Installing the Initial Policy

To be able to inspect traffic, the sensors and analyzers must have an IPS policy installed on them. Installing one of the predefined IPS policies provides an easy way to begin using the IPS system. You can then fine-tune the system as needed. The system has the following ready-made IPS Policies:

Table 7.1 Default IPS Policies

IPS Policy	Description
Strict Policy	Contains the predefined rules inherited from the IPS Strict Template. Suitable as the initial policy in high-risk environments, such as data centers. Recommended only for use with inline sensors.
System Policy	Contains the predefined rules inherited from the IPS System Template. Suitable as the initial policy in most network environments.
Certification Policy	This policy was used when StoneGate IPS was tested at NSS Labs. We recommend that you install either the Strict Policy or the System Policy as the initial policy on the IPS engines.

The Strict Policy and the System Policy are added and updated when you import new dynamic updates (see the Management Client *Online Help* or the *Administrator's Guide* PDF for more information). Because of this, the Strict Policy, IPS Strict Template, System Policy, and IPS System Template cannot be edited directly. See the *IPS Reference Guide* for more information on the predefined policies and templates.

When you install a policy on a sensor, the analyzer that the sensor uses also receives a new policy. You do not install the policy separately on analyzers.

▼ To install the Strict Policy or the System Policy

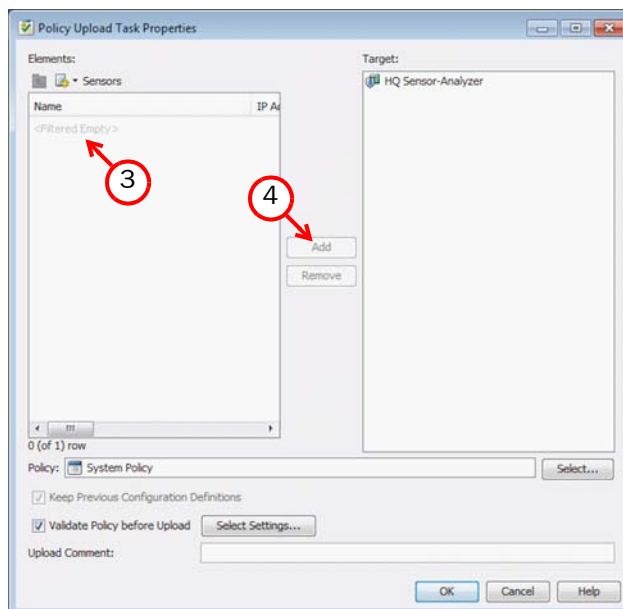
1. Click the Configuration icon in the toolbar and select **IPS**. The IPS Configuration view opens with the IPS Policies branch expanded.



2. Right-click **Strict Policy** or **System Policy** and select **Install Policy**. The Policy Install task dialog opens.

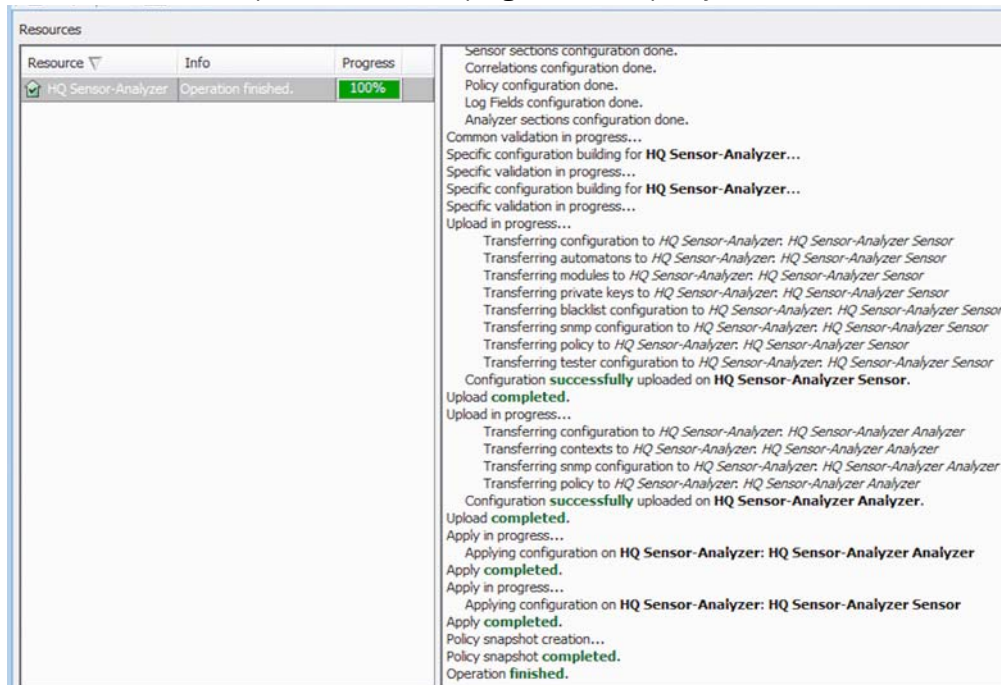


Note – The **Strict Policy** and the **System Policy** contain a rule that uses the **Terminate** action for an **Analyzer-only Situation**. This produces an **Unsupported Definitions** issue during validation, but does not affect the functioning of the system.



3. Select the engine(s).
4. Click **Add**. The selected engines are added to the Target list.

5. Click **OK**. A new tab opens to show the progress of the policy installation.



6. Check that the policy installation is successful for both the sensor and the analyzer.

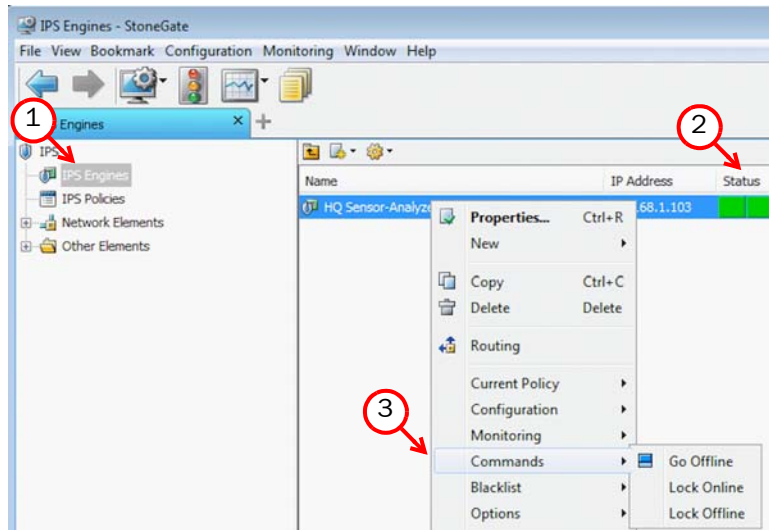
When you install a policy, all the rules in the policy as well as all the IPS engine's other configuration information (including interface definitions and routing information) are transferred to the engines.

Commanding IPS Engines

After a successful policy installation, your system is ready to process traffic. You can control the sensors and analyzers using the right-click menu as shown in the illustration below.

▼ To check system status and issue commands to sensors and analyzers

1. Select **IPS Engines**.



2. Check the status of the engines in the **Status** column. You can select an element to view more information about it in the **Info** panel at the bottom of the window.

3. Use the **Commands** menu to command sensors Online/Offline. Only sensors in **Online** mode process traffic. Analyzers do not have a corresponding command: they always process the event information that any online sensors send them.

This concludes the configuration instructions in this *Installation Guide*. To continue setting up your system, consult the *Online Help* (or the *Administrator's Guide* PDF), particularly the *Introduction to StoneGate* in the *Getting Started* section.

INSTALLING SENSORS AND ANALYZERS

In this section:

[Installing the Engine on Intel-Compatible Platforms - 61](#)

CHAPTER 8

INSTALLING THE ENGINE ON INTEL-COMPATIBLE PLATFORMS

This chapter describes how to install StoneGate IPS Sensors and Analyzers on standard Intel or Intel-compatible platforms, such as AMD.

The following sections are included:

- ▶ [Installing the Sensor or Analyzer Engine](#) (page 62)
- ▶ [Obtaining Installation Files](#) (page 62)
- ▶ [Starting the Installation](#) (page 63)
- ▶ [Configuring the Engine](#) (page 64)
- ▶ [Installing the Engine in Expert Mode](#) (page 70)

Installing the Sensor or Analyzer Engine

StoneGate hardware appliances are delivered with pre-installed software. If you are using a StoneGate appliance, configure the software as instructed in the *Appliance Installation Guide* delivered with the appliance.

On other systems, the software is installed from CD-ROMs. Depending on your order, you may have received ready-made Management Center and IPS engine CD-ROMs. If the CD-ROMs are not included in the order, you will first have to create them.

The installation steps for a Sensor, Analyzer, and combined Sensor-Analyzer are similar, as the engine type is only selected at the end of the installation.



Caution – Check that the Automatic Power Management (APM) and Advanced Configuration and Power Interface (ACPI) settings are disabled in BIOS. Otherwise, the engine may not start after installation or may shut down unexpectedly.



Note – The engines must be dedicated to StoneGate IPS. No other software can be installed on them.

Configuration Overview

1. If you do not have ready-made installation CD-ROMs, obtain the files from the Stonesoft website. See [Obtaining Installation Files](#) (page 62).
2. Start the installation and select the installation type. See [Starting the Installation](#) (page 63).
3. Configure the engines and establish contact with the Management Server. See [Configuring the Engine](#) (page 64).

What's Next?

- ▶ If you have ready-made CD-ROMs, proceed to [Starting the Installation](#) (page 63).
- ▶ Otherwise, start by [Obtaining Installation Files](#).

Obtaining Installation Files

Downloading the Installation Files

1. Go to the download page at the Stonesoft website: <https://my.stonesoft.com/download>
2. Download the .iso image files.

Checking File Integrity

Before installing StoneGate from downloaded files, check that the installation files have not become corrupt or been modified. Using corrupt files may cause problems at any stage of the installation and use of the system. File integrity is checked by generating an MD5 or SHA-1 file checksum of the downloaded files and by comparing the checksum with the checksum on the download page at the Stonesoft website.

Windows does not have MD5 or SHA-1 checksum tools by default, but there are several third-party programs available.

▼ To check MD5 or SHA-1 file checksum

1. Look up the correct checksum at <https://my.stonesoft.com/download/>.
2. Change to the directory that contains the file(s) to be checked.
3. Generate a checksum of the file using the command `md5sum filename` or `sha1sum filename`, where *filename* is the name of the installation file.
4. Compare the displayed output to the checksum on the website. They must match.



Caution – Do not use files that have invalid checksums. If downloading the files again does not help, contact Stonesoft technical support to resolve the issue.

Creating the Installation CD-ROM

Once you have checked the integrity of the installation files, create the installation CD-ROM from the files. Use a CD-burning application that can correctly read and burn the CD-structure stored in the `.iso` images. If the end result is a CD-ROM file with the original `.iso` file on it, the CD-ROM cannot be used for installation.

Starting the Installation

Before you start installing the engines, make sure you have the initial configuration or a one-time password for management contact for each sensor and analyzer engine. These are generated in the Management Center. See [Saving the Initial Configuration for Sensors and Analyzers](#) (page 46) for more information.

What you see on your screen during the installation may differ from the illustrations in this guide depending on your system configuration.



Caution – Installing StoneGate deletes all existing data on the hard disk.

▼ To install StoneGate engine from a CD-ROM

1. Insert the StoneGate engine installation CD-ROM into the drive and reboot the machine. The License Agreement appears.
2. Type `YES` and press `ENTER` to accept the license agreement and continue with the configuration.

```
StoneGate Engine Installation System
Existing StoneGate installation has not been detected.
1. Full install
2. Full install in expert mode
Enter your choice:
```

3. Select the type of installation: **Full Install** and **Full Install in expert mode**.
 - Type **1** for the normal **Full Install**.
 - Type **2** for the **Full Install in expert mode** if you want to partition the hard disk manually, and continue in [Installing the Engine in Expert Mode](#) (page 70).

4. Enter the number of processors:
 - For a uniprocessor machine, type 1 and press ENTER.
 - For a multiprocessor machine, type 2 and press ENTER.
5. Type **YES** and press ENTER to accept automatic hard disk partitioning. The installation process starts.
 - If you want to use the automatic configuration method, do not reboot once the installation finishes. Continue in [Configuring the Engine Automatically with a USB Stick](#) below.
 - Otherwise, remove the CD-ROM and press ENTER to reboot when prompted to do so. The Configuration Wizard starts. Continue in [Configuring the Engine in the Engine Configuration Wizard](#) (page 65).

Configuring the Engine

Configuring the Engine Automatically with a USB Stick

The automatic configuration is primarily intended to be used with StoneGate appliances, and may not work in all environments when you use your own hardware. If the automatic configuration does not work, you can still run the Configuration Wizard as explained in the next section and import or enter the information manually.

When automatic configuration is used, Interface IDs are mapped to physical interfaces in sequential order: Interface ID 0 is mapped to eth0, Interface ID 1 is mapped to eth1, and so on.



Note – The imported configuration does not contain a password for the root account on the engine, so you must set the password manually in the Management Client before you can log in for command line access to the engine. See the *Online Help of the Management Client* or the *StoneGate Administrator's Guide PDF* for more information.

▼ To install and configure the engine with a USB stick

1. Make sure you have a physical connection to the appliance using a monitor and keyboard or a serial cable.
2. Insert the USB stick.
3. Remove the CD-ROM and press ENTER at the installation finished prompt. The engine reboots, imports the configuration from the USB stick, and makes initial contact to the Management Server.
 - If the automatic configuration fails, and you do not have a display connected, you can check for the reason in the log (`sg_autoconfig.log`) written on the USB stick.
 - If you see a “connection refused” error message, ensure that the Management Server IP address is reachable from the node.

The configuration is complete when the engine successfully contacts the Management Server and reboots itself.

What's Next?

- ▶ Continue the configuration in [After Successful Management Server Contact](#) (page 70).

Configuring the Engine in the Engine Configuration Wizard

If you have stored the configuration on a floppy disk or a USB memory stick (see [Saving the Initial Configuration for Sensors and Analyzers](#) (page 46)), you can import it to reduce the need for typing in information.

▼ To select the configuration method

- To import a saved configuration, highlight **Import** using the arrow keys and press ENTER. Otherwise, highlight **Next** and press ENTER. Proceed to [Configuring the Operating System Settings](#) (page 65).



▼ To import the configuration

1. Select **Floppy Disk** or **USB Memory** and press ENTER.

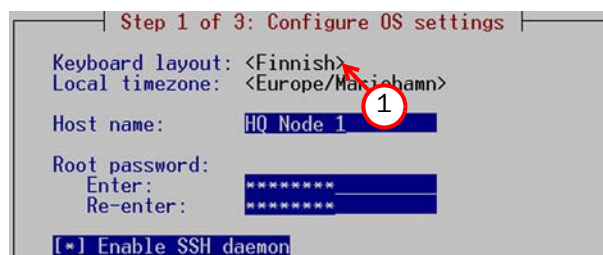


2. Select the correct configuration file for this engine.
3. Highlight **Next** and press ENTER to continue.

Configuring the Operating System Settings

▼ To set the keyboard layout

1. Highlight the entry field for **Keyboard Layout** using the arrow keys and press ENTER. The Select Keyboard Layout dialog opens.



2. Highlight the correct layout and press ENTER. Type the first letter to move forward more quickly.

If the desired keyboard layout is not available, use the best-matching available layout, or select US_English.

▼ To set the engine's timezone

1. Highlight the entry field for **Local Timezone** using the arrow keys and press ENTER.

```
Step 1 of 3: Configure OS settings
Keyboard layout: <Finnish>
Local timezone: <Europe/Mariehamn>
Host name:      HQ Node 1
Root password:
Enter:          *****
Re-enter:      *****
[*] Enable SSH daemon
```

2. Select the correct timezone in the dialog that opens.

The timezone setting only affects the way the time is displayed on the engine command line. The engine always uses UTC time. The engine's clock is automatically synchronized with the Management Server's clock.

▼ To set the rest of the OS settings

1. Type in the name of the engine.
2. Type in the password for the user `root`. This is the only account for engine command line access.

```
Step 1 of 3: Configure OS settings
Keyboard layout: <Finnish>
Local timezone: <Europe/Mariehamn>
Host name:      HQ Node 1
Root password:
Enter:          *****
Re-enter:      *****
[*] Enable SSH daemon
<<-Back>      <Next->>
```

3. (Optional) Highlight **Enable SSH Daemon** and press the spacebar to allow remote access to engine command line using SSH.



Note – Unless you have a specific need to enable SSH access to the engine command line, we recommend leaving it disabled.

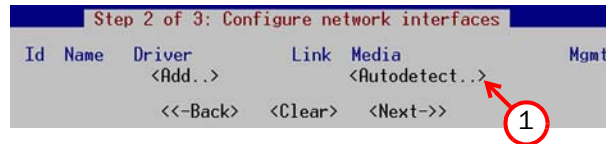
4. Highlight **Next** and press ENTER. The Configure Network Interfaces page opens.

Configuring the Network Interfaces

The Configuration Wizard can automatically detect which network cards are in use. You can also add interfaces manually if necessary. If the list is not populated automatically, you can launch the autodetect as explained in the illustration below.

▼ To add the network interfaces

- Highlight **Autodetect** and press ENTER.



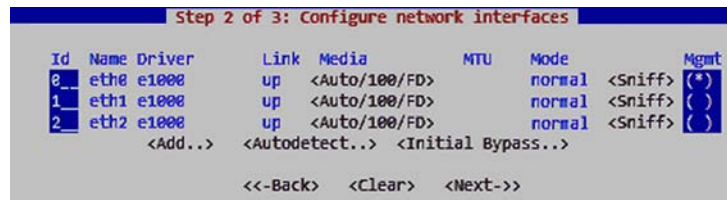
Check that the detected drivers are correct and that all interfaces have been detected.

What's Next?

- ▶ If there are problems, add the network interfaces manually as explained in [To define the network interface drivers manually](#) (page 68).
- ▶ Otherwise, proceed to [To map the physical interfaces to Interface IDs](#).

▼ To map the physical interfaces to Interface IDs

1. Change the **IDs** as necessary to define how physical interfaces are mapped to the interface IDs you defined in the Sensor or Analyzer element.



2. If necessary, highlight the **Media** column and press ENTER to match the speed/duplex settings to those used in each network.

Tip – You can use the **Sniff** option to troubleshoot the network interfaces. Select **Sniff** on an interface to run the network sniffer on that interface

3. Highlight the **Mgmt** column and press the spacebar to select the interface for contact with the Management Server.



Note – The Management interface must be the same interface that is configured as the Management Interface for the corresponding engine element in the Management Center.

4. (Optional, sensors and sensor-analyzers only) Highlight **Initial Bypass** and press ENTER if you want to set your sensor or sensor-analyzer temporarily to the initial bypass state and define one or more soft-bypass interface pairs through which traffic flows.
 - Setting the appliance to the initial bypass state can be useful during IPS appliance deployment if bypass network interface pairs on the appliance are in the Normal mode. Initial bypass allows traffic to flow through the IPS appliance until the initial configuration

is ready and an IPS policy is installed on the appliance. Do not set the initial bypass state when the bypass network interface pairs are in the Bypass mode.

- In the illustration below, interface 1 is soft-bypassed with interface 2.

Id	Name	Driver	Link	Pair	Id
1	eth1	e1000	up	2	
2	eth2	e1000	up	1	

<Cancel> <OK>

5. Highlight **Next** and press ENTER to continue.

What's Next?

- ▶ Proceed to [Contacting the Management Server](#) (page 68).

▼ To define the network interface drivers manually

1. Highlight **Add** and press ENTER.

Id	Name	Driver	Link	Media	Mgmt
		<Add..>		<Autodetect..>	

<<-Back> <Clear> <Next->

2. Select a driver that is used for your network card(s) and press ENTER.

Repeat as necessary, then map the interfaces to Interface IDs as explained above.

Contacting the Management Server

The Prepare for Management Contact page opens. If the initial configuration was imported, most of this information is automatically filled in.

Activating the Initial Configuration

Before the engine can make initial contact with the Management Server, you activate an initial configuration on the engine. The initial configuration contains the information that the engine needs to connect to the Management Server for the first time.

▼ To activate the Initial Configuration

1. Highlight **Switch Node to Initial Configuration** and press the spacebar.

```
[ ] Switch to initial configuration
IP address:* 192.168.10.15
Netmask:* 255.255.255.0
Gateway to management: _____
[ ] Use VLAN, Identifier: _____
```

2. Fill in according to your environment. The information must match to what you defined for the engine element (Primary Control IP Address). If the engine and the Management Server are on the same network, you can leave the **Gateway to Management** field empty.

The initial configuration does not contain any working IPS policy. You must install an IPS policy on the engine using the Management Client to make it operational.

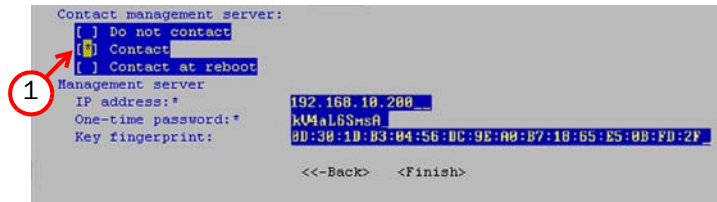
Filling in the Management Server Information

In the second part of the configuration, you define the information needed for establishing a trust relationship between the engine and the Management Server.

If you do not have a one-time password for this engine, see the [Saving the Initial Configuration](#) (page 45).

▼ To fill in the Management Server information

1. Select **Contact** or **Contact at Reboot** and press the spacebar.



```
Contact management server:
[ ] Do not contact
[ ] Contact
[ ] Contact at reboot
Management server
IP address:* 192.168.10.200
One-time password:* kUMaL6SmsR
Key fingerprint: 8D:38:1D:83:84:56:0C:9E:A8:B7:18:65:E5:08:FD:2F
<<-Back> <Finish>
```

2. Enter the Management Server IP address and the one-time password.
3. (Optional) Fill in the Key fingerprint (also shown when you saved the initial configuration). This increases the security of the communications.



Note – The one-time password is engine-specific and can be used only for one initial connection to the Management Server. Once initial contact has been made, the engine receives a certificate from the Management Server for identification. If the certificate is deleted or expires, you must repeat the initial contact using a new one-time password.

Selecting the Engine Type

In the third part of the configuration, you select whether you want this engine to work as a Sensor, an Analyzer, or a combined Sensor-Analyzer. The selection you make must correspond to the element you created for this engine in the Management Client.

▼ To select the engine type

1. Select the type of engine using the arrow keys and the spacebar.



```
(*) Install Sensor
( ) Install Analyzer
( ) Install Combo (sensor+analyzer)
<<-Back> <Finish>
```

2. Highlight **Finish** and press ENTER.

The engine now tries to make initial Management Server contact.

- If you see a “connection refused” error message, ensure that the one-time password is correct and the Management Server IP address is reachable from the node. Save a new initial configuration if you are unsure about the password.
- If there is a firewall between the engine and the Management Server or Log Server, make sure that the firewall’s policy allows the initial contact and the subsequent communications. See [Default Communication Ports](#) (page 95) for a list of the ports and protocols used.

If the initial management contact fails for some reason, the configuration can be started again with the `sg-reconfigure` command.

After Successful Management Server Contact

After you see a notification that Management Server contact has succeeded, the IPS engine installation is complete and the engine is ready to receive a policy. The engine element's status changes in the Management Client from **Unknown** to **No Policy Installed**, and the connection state is **Connected**, indicating that the Management Server can connect to the node.

What's Next?

- ▶ To finish the engine configuration, proceed to [Configuring Routing and Installing Policies](#) (page 51).

Installing the Engine in Expert Mode

To start the installation, reboot from the CD-ROM (see [Installing the Sensor or Analyzer Engine](#) (page 62)).

The difference between the normal and expert installation is that in expert mode, you partition the hard disk manually. If you are unfamiliar with partitioning hard disks in Linux, we recommend that you use the normal installation process.



Caution – When using the command prompt, use the `reboot` command to reboot and `halt` command to shut down the node. Do not use the `init` command. You can also reboot the node using the Management Client.

Partitioning the Hard Disk Manually

Typically, you need five partitions for the StoneGate IPS Sensor or Analyzer as explained in [Table 8.1](#). The partitions are allocated in two phases. First, disk partitions are created and second, the partitions are allocated for their use purposes.



Caution – Partitioning deletes all the existing data on the hard disk.

▼ To partition the hard disk

1. If you are asked whether you want to create an empty partition table, type `y` to continue.
2. When prompted, press `ENTER` to continue. The partition table is displayed.
3. Create the partitions for the engine as follows:

Table 8.1 Partitions for the Engine

Partition	Flags	Partition Type	Filesystem Type	Size	Description
Engine root A	bootable	Primary	Linux	200 MB	The bootable root partition for the StoneGate IPS engine.
Engine root B		Primary	Linux	200 MB	Alternative root partition for the StoneGate IPS engine. Used for the engine upgrade.

Table 8.1 Partitions for the Engine (Continued)

Partition	Flags	Partition Type	Filesystem Type	Size	Description
Swap		Logical	Linux swap	Twice the size of physical memory.	Swap partition for the StoneGate IPS engine.
Data		Logical	Linux	500 MB or more	Used for the boot configuration files and the root user's home directory.
Spool		Logical	Linux	All remaining free disk space.	Used for spooling

4. Check that the partition table information is correct.
5. Select **Write** to commit the changes and confirm by typing **yes**.
6. Select **Quit** and press ENTER.

Allocating Partitions

After partitioning the hard disk, the partitions are allocated for the StoneGate IPS engine.

▼ To allocate the partitions

1. Check that the partition table is correct. Type **yes** to continue.
2. Using the partition numbers shown in the partition table, assign the partitions for the engine, for example:
 - For the engine root A partition, type 1.
 - For the engine root B partition, type 2.
 - For the swap partition, type 5.
 - For the data partition, type 6.
 - For the spool partition, type 7.
3. Check the partition allocation and type **yes** to continue. The engine installation starts.
4. When installation is complete, remove the CD-ROM from the machine and press ENTER to reboot.

What's Next?

- ▶ Continue the configuration as described in [Configuring the Engine](#) (page 64).

UPGRADING

In this section:

[Upgrading - 75](#)

CHAPTER 9

UPGRADING

This chapter explains how you can upgrade your IPS engines. When there is a new version of the sensor and analyzer engine software, you should upgrade as soon as possible.

The following sections are included:

- ▶ [Getting Started with Upgrading](#) (page 76)
- ▶ [Upgrading or Generating Licenses](#) (page 78)
- ▶ [Upgrading Engines Remotely](#) (page 82)
- ▶ [Upgrading Engines Locally](#) (page 84)

Getting Started with Upgrading

How Engine Upgrades Work

The primary way to upgrade engines is a remote upgrade through the Management Server. The upgrade package is imported on the Management Server manually or automatically. Then, you apply it to selected engines through the Management Client. Alternatively, the upgrade can be done locally when it is more convenient (for example, for spare appliances in storage).

The engines have two alternative partitions for the engine software. When you install a new software version, it is installed on the inactive partition and the current version is preserved to allow rollback to the previous version in case the installation is interrupted or some other problems arise. If the engine is not able to return to operation, it automatically returns to the previous software version at the next reboot. You can also switch the active partition manually. You can upload and activate the new software separately, for example, to upload the upgrade during office hours but activate it during a service window.

The currently installed working configuration (routing, policies etc.) is stored separately and is not changed in an upgrade or a rollback. Although parts of the configuration may be version-specific (for example, if system communications ports are changed), the new version can use the existing configuration. Possible version-specific adjustments are made when you refresh the policy after the upgrade.

What Do I Need to Know before I Begin

The Management Center must be up to date before you upgrade the engines. An old Management Center version may not be able to recognize the new version engines and generate a valid configuration for them. Several older versions of engines can be controlled by any newer Management Center versions. See the [Release Notes](#) for version-specific compatibility information.

During a cluster upgrade, it is possible to have the upgraded nodes online and operational side by side with the older version nodes. This way, you can upgrade the nodes one by one while the other nodes handle the traffic. However, you must upgrade all the nodes to the same version as soon as possible, as prolonged use with mismatched versions is not supported.

To check the current engine software version, select the engine in the System Status view. The engine version is displayed on the General tab in the Info panel. If the Info panel is not shown, select **View**→**Info**.

Before upgrading the engines, read the [Release Notes](#) for the new engine version.

Configuration Overview

Proceed as follows with the engine upgrade:

1. (If automatic download of engine upgrades has been disabled) Obtain the installation files and check the installation file integrity (see [Obtaining Installation Files](#) (page 77)).
2. (If you are upgrading engines locally) Create the installation CD-ROMs from the files with a CD-burning application that can correctly read and burn the CD-structure stored in the `.iso` images.
3. (If automatic license updates have been disabled) Update the licenses (see [Upgrading or Generating Licenses](#) (page 78)).
4. Upgrade the sensor and analyzer engines one by one. Confirm that the upgraded engine operates normally before upgrading the next engine (see [Upgrading Engines Remotely](#) (page 82) or [Upgrading Engines Locally](#) (page 84)).

Obtaining Installation Files

If the Management Server is not set up to download engine upgrades automatically or if you want to perform a local upgrade, you must download the installation files manually and check the installation file integrity using the MD5 or SHA-1 file checksums. Windows does not have MD5 or SHA-1 checksum programs by default, but there are several third party programs available.

▼ To manually download an engine upgrade file

1. Download the installation file from www.stonesoft.com/download/. There are two types of packages available:
 - The `.zip` package is used in the remote upgrade on all supported platforms. It can also be used for a local upgrade from a USB memory stick or a non-bootable CD-ROM.
 - The `.iso` download allows you to create a bootable installation CD-ROM for a local upgrade on all supported platforms.
2. Change to the directory that contains the file(s) to be checked.
3. Generate a checksum of the file using the command `md5sum filename` or `sha1sum filename`, where `filename` is the name of the installation file.

Example

```
$ md5sum sg_engine_1.0.0.1000.iso
869aec7dc39321aa2e0cfaf7fafdb8f sg_engine_1.0.0.1000.iso
```

4. Compare the displayed output to the checksum on the website.



Caution – Do not use files that have invalid checksums. If downloading the files again does not help, contact Stonesoft technical support to resolve the issue.

▼ To prepare a downloaded ZIP file for a remote upgrade

1. Log in to the Management Client and select **File**→**Import**→**Import Engine Upgrades** from the top menu.
2. Select the engine upgrade (`sg_engine_version_platform.zip` file) and click **Import**. The import takes a while. You can see the related messages in the status bar at the bottom of the Management Client window.

▼ To prepare a downloaded ZIP file for a local upgrade

- ➔ Copy the file to the root directory of a USB memory stick or on a CD-ROM.

▼ To prepare a downloaded ISO file for a local upgrade

- ➔ Create the installation CD-ROM for the engines with a CD-burning application that can correctly read and burn the CD-structure stored in the `.iso` images. If the end result is a CD-ROM file with the original `.iso` file on it, the CD-ROM cannot be used for installation.

What's Next?

- ▶ If you are sure you do not need to upgrade your licenses, you are ready to upgrade the sensor and analyzer engines. Continue by [Upgrading Engines Remotely](#) (page 82), or [Upgrading Engines Locally](#) (page 84) depending on whether you are going to upgrade the engines remotely through the Management Server or locally at the engine site.
- ▶ Otherwise, continue by [Upgrading or Generating Licenses](#).

Upgrading or Generating Licenses

When you installed StoneGate for the first time, you installed licenses that work with all versions of StoneGate up to that particular version. If the first two numbers in the old and the new version are the same, the upgrade can be done without upgrading licenses (for example, when upgrading from 1.2.3 to 1.2.4). When either of the first two numbers in the old version and the new version are different, you must first upgrade your licenses (for example, when upgrading from 1.2.3 to 1.3.0). By default, licenses are regenerated and installed automatically. You can also upgrade the licenses at the Stonesoft website.

What's Next?

- ▶ If you do not need to upgrade licenses and you want to upgrade the sensor and analyzer engines remotely through the Management Server, proceed to [Upgrading Engines Remotely](#) (page 82).
- ▶ If you do not need to upgrade licenses and you want to upgrade the engines locally at the engine site, proceed to [Upgrading Engines Locally](#) (page 84).
- ▶ If you need new licenses and you want to upgrade the licenses one by one, proceed to [Upgrading Licenses Under One Proof Code](#) (page 78).
- ▶ If you need new licenses and you want to upgrade several licenses at once, Proceed to [Upgrading Licenses Under Multiple Proof Codes](#) (page 79).

Upgrading Licenses Under One Proof Code

A license file generated under one POL code contains the license information for several components. You can also always use the multi-upgrade form to upgrade the licenses (see [Upgrading Licenses Under Multiple Proof Codes](#) (page 79)).

▼ To generate a new license

1. Browse to the Stonesoft License Center at www.stonesoft.com/license/.
2. Enter the POL code in the **License Identification** field and click **Submit**. The license page opens.

3. Click **Update**. The license upgrade page opens.
4. Follow the directions on the page that opens to upgrade the license.

Repeat for other licenses.

What's Next?

- ▶ Proceed to [Installing Licenses](#) (page 80).

Upgrading Licenses Under Multiple Proof Codes

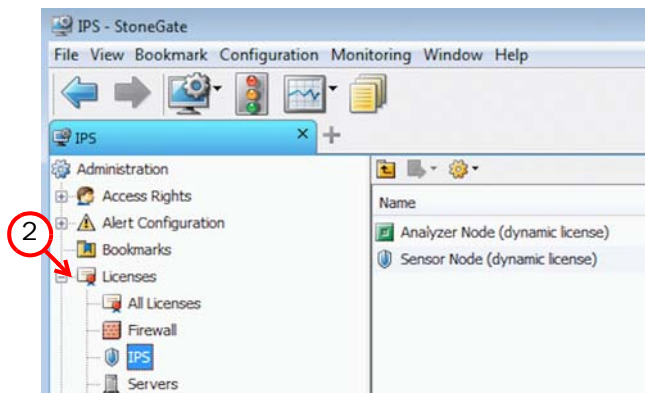
If you have several existing licenses with different POL codes that you need to upgrade, you can make the work easier by generating the new licenses all at once.

▼ To upgrade multiple licenses

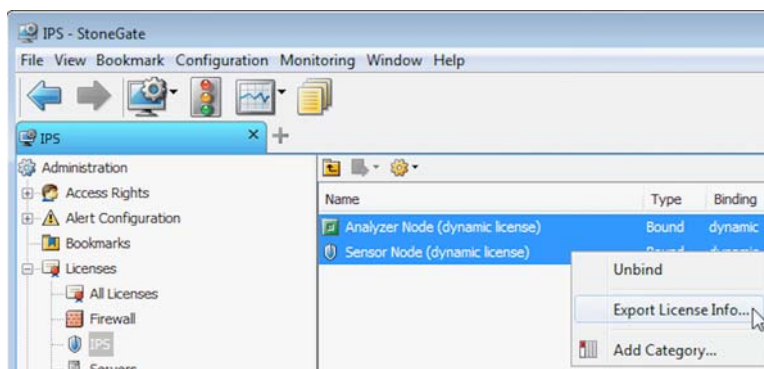
1. Click the Configuration icon in the toolbar and select **Administration**. The Administration Configuration view opens.



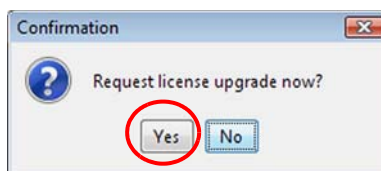
2. Expand the **Licenses** branch and select **IPS**.



3. Ctrl-select or Shift-select the licenses you want to upgrade.



4. Right-click one of the selected items and select **Export License Info**.
5. Select the location where the license file is saved in the dialog that opens. You are prompted to request a license upgrade.



6. (Optional) Click **Yes** to launch the Stonesoft License Center website's multi-upgrade form in your default Web browser.

Next, upload the license upgrade request file to the Stonesoft License Center website using the multi-upgrade form, and submit the form with the required details. The upgraded licenses are sent to you.

You can view and download your current licenses at the license website (log in by entering the proof-of-license or proof-of-serial number code at the License Center main page).

Installing Licenses

After you have generated the licenses for the upgrade as described above, you install the license file in the Management Client.

▼ To install StoneGate licenses

1. Select **File**→**System Tools**→**Install Licenses**.



2. Select one or more license files to install in the dialog that opens. The new licenses are now installed.

Checking the Licenses

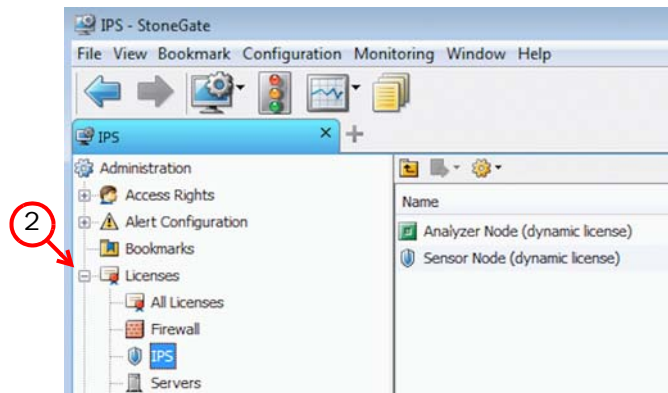
After installing the upgraded licenses, check the license information. When you upgrade licenses, the old licenses are automatically replaced with the new licenses.

▼ To check the licenses

1. Click the Configuration icon in the toolbar and select **Administration**. The Administration Configuration view opens.



2. Expand the **Licenses** branch and select **IPS**. You should see one license for each analyzer and sensor engine.



What's Next?

- ▶ If you want to upgrade the sensor and analyzer engines remotely through the Management Server, proceed to [Upgrading Engines Remotely](#) (page 82).
- ▶ If you want to upgrade the engines locally at the engine site, proceed to [Upgrading Engines Locally](#) (page 84).

Upgrading Engines Remotely

The remote upgrade has two separate parts, transfer and activation. You can choose to do both parts consecutively, or you can choose to transfer the configuration now and then launch a separate task for the activation at a later time. You can also create a scheduled Task for the remote upgrade as instructed in the *Online Help*.

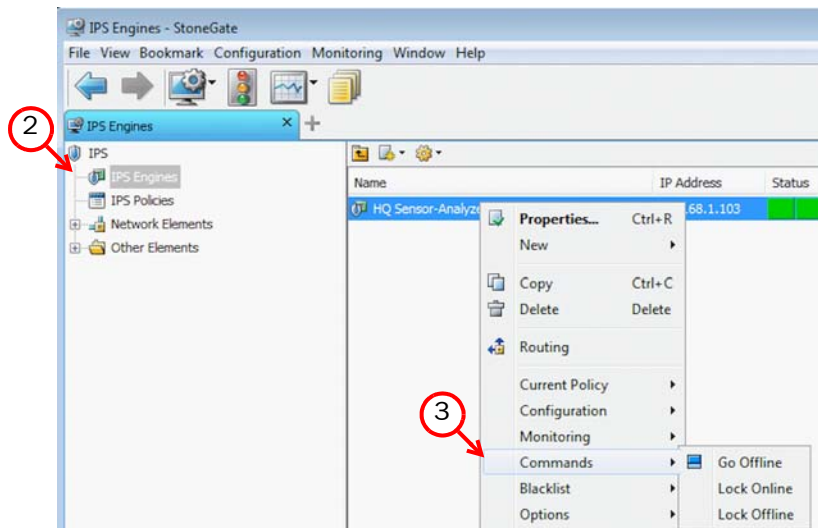
During a Sensor cluster upgrade process, it is possible to have the upgraded nodes online and operational side by side with the older version nodes. For full functionality, you must upgrade all the nodes to the same version as soon as possible.

▼ To upgrade the engine

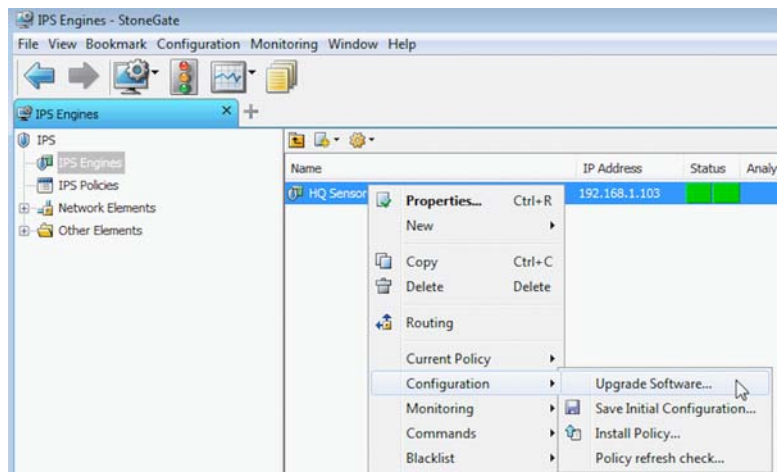
1. Click the Configuration icon in the toolbar and select **Administration**. The Administration Configuration view opens.



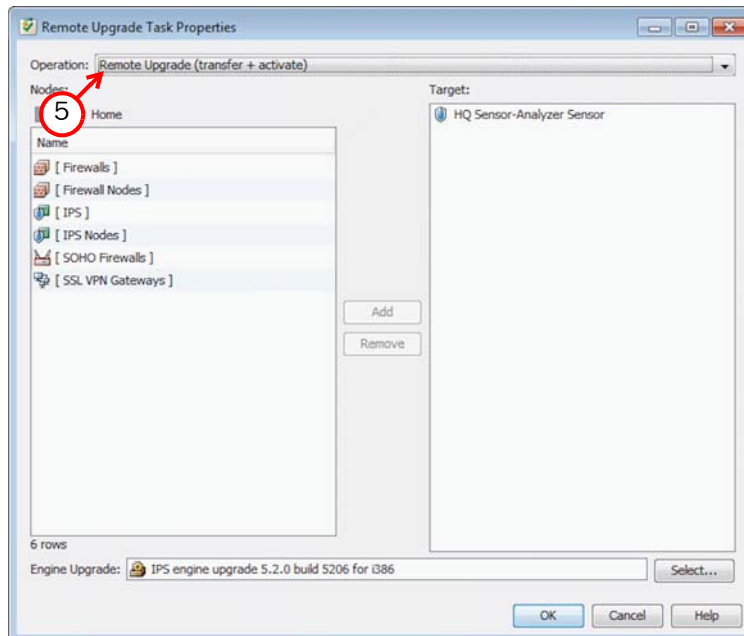
2. Select **IPS Engines**.



3. (Sensors only) If you want to activate the new version immediately (and not only transfer it), right-click the sensor node and select **Commands**→**Go Offline**.



4. Right-click the node and select **Configuration**→**Upgrade Software**.



5. Select whether you want to transfer the upgrade for later activation, or both transfer and activate now.
6. Check the node selection and change it, if necessary.
7. Check the **Engine Upgrade** file and change it, if necessary.
8. Click **OK**.

A new tab opens showing the progress of the upgrade. The time it takes to upgrade the node varies depending on the performance of your machine and the network environment. Click **Abort** if you want to stop the upgrade.

If you chose to activate the new configuration, once the engine is successfully upgraded, the machine is automatically rebooted and the upgraded engine is brought to the online state.

If you are upgrading a Sensor cluster, we recommend beginning the upgrade on the next node only when the upgraded node is back online. StoneGate operates normally with two different versions of the engines online during the upgrade.

Note that the engines have two partitions. When an engine is upgraded, the inactive partition is used. When the upgrade is finished, the active partition is switched. The earlier configuration is kept on the inactive partition. If there is an error during the upgrade, you can use the `sg-toggle-active` command to roll back to the previous engine version. See [Command Line Tools](#) (page 89) for more information.

What's Next?

- ▶ The upgrade is now complete.

Upgrading Engines Locally

It is also possible to upgrade the engines locally at the engine site as described in this section. Upgrading locally requires a physical connection to the engine using a monitor and keyboard or a serial cable.

During a Sensor cluster upgrade process, it is possible to have the upgraded nodes online and operational side by side with the older version nodes.

What's Next?

- ▶ If the hardware has a CD drive (a USB CD-ROM drive can be used) and you have a full StoneGate installation CD-ROM, proceed to [Upgrading from an Engine Installation CD-ROM](#).
- ▶ if you want to upgrade from a `.zip` archive file on a USB stick or on a CD-ROM, proceed to [Upgrading from a ZIP Archive File](#) (page 85).

Upgrading from an Engine Installation CD-ROM

Follow the procedure below to upgrade StoneGate engines to the latest version locally from a CD-ROM that you have created from an `.iso` image downloaded from the Stonesoft website or shipped to you by Stonesoft.

▼ To upgrade the engine from an engine installation CD-ROM

1. (*Recommended*) Log in to the node as `root` with the password you set for the engine (you can set the password through the Management Client).
2. Insert the StoneGate engine installation CD-ROM into the engine's CD drive.
3. Reboot the node from the CD-ROM with the command `reboot` (*recommended*) or by cycling the power (if you cannot log in). You are prompted to select the upgrade type.

```

StoneGate Engine Installation System

An existing StoneGate Engine installation has been detected.

1. Upgrade existing installation
2. Re-install using configuration from existing installation
3. Full re-install (old configuration is not preserved)
4. Full re-install in expert mode

Enter your choice: _

```

4. Select **1** to upgrade the previous installation and press **ENTER** to continue. The upgrade process starts.
5. When the process is finished, remove the CD-ROM and press **ENTER** to reboot.
 - If the Configuration Wizard opens, configure the engine in the same way as after the first installation: refer to [Configuring the Engine](#) (page 100) for instructions.
6. When the upgrade is finished, right-click the node in the Management Client and select **Commands**→**Go Online**. The node can also be brought online with the command `sg-cluster online` on the engine command line.

If you are upgrading a Sensor cluster, we recommend beginning the upgrade on the next node only when the upgraded node is back online. StoneGate operates normally with two different versions of the engines online during the upgrade.

Note that the engines have two partitions. When an engine is upgraded, the inactive partition is used. When the upgrade is finished, the active partition is switched. The earlier configuration is kept on the inactive partition. If there is an error during the upgrade, you can use the `sg-toggle-active` command to roll back to the previous engine version. See [Command Line Tools](#) (page 129) for more information.

What's Next?

- ▶ The upgrade is now complete.

Upgrading from a ZIP Archive File

Follow the instructions below if you do not want to use the remote upgrade, but you want to use a `.zip` archive to upgrade the firewall software.

▼ To upgrade the engine locally from an archive file

1. (Recommended) Log in to the node as root with the password set for the engine (you can set the password through the Management Client).
2. Insert the USB stick or the CD-ROM.
3. Run the command `sg-reconfigure`. The engine Configuration Wizard opens.
4. Select **Upgrade** using the arrow keys and press **ENTER**.



5. Select the source media where the upgrade file is located.

6. (Optional) If you have not already done so, select **Calculate SHA1** to calculate the checksum. The calculation will take some time. The calculated checksum must be identical to the one from the `.zip` file.



Caution – Do not use files that have invalid checksums. Select **Cancel if the checksum does not match and acquire a new copy of the upgrade file.**

7. Select **OK**. The software is upgraded.
8. When prompted, press ENTER. The engine reboots to the new version.

Note that the engines have two partitions. When an engine is upgraded, the inactive partition is used. When the upgrade is finished, the active partition is switched. The earlier configuration is kept on the inactive partition. If there is an error during the upgrade, you can use the `sg-toggle-active` command to roll back to the previous engine version. See [Command Line Tools](#) (page 129) for more information.

What's Next?

- ▶ The upgrade is now complete.

APPENDICES

In this section:

Command Line Tools - 89

Default Communication Ports - 95

Example Network Scenario - 101

Index - 107

APPENDIX A

COMMAND LINE TOOLS

This appendix describes the command line tools available on StoneGate IPS engines. For instructions on how to access the command line, see the *Administrator's Guide* or the *Online Help* of the Management Client.

The following sections are included:

- ▶ [StoneGate-Specific Commands](#) (page 90)
- ▶ [General Tools](#) (page 93)

StoneGate-Specific Commands

StoneGate engine commands can be run from the command line on the sensors and analyzers. For a full list of command line tools for all types of components, see the *Command Line Tools* appendix in the *Administrator's Guide* or the *Online Help* of the Management Client.

Table A.1 StoneGate-specific Command Line Tools on Engines

Command	Description
<pre> sg-blacklist show [-v] [-f <i>FILENAME</i>] add [[-i <i>FILENAME</i>] [src <i>IP_ADDRESS/MASK</i>] [dst <i>IP_ADDRESS/MASK</i>] [proto {<i>tcp udp icmp NUM</i>}] [srcport <i>PORT</i>{-<i>PORT</i>}] [dstport <i>PORT</i>{-<i>PORT</i>}] [duration <i>NUM</i>]] del [[-i <i>FILENAME</i>] [src <i>IP_ADDRESS/MASK</i>] [dst <i>IP_ADDRESS/MASK</i>] [proto {<i>tcp udp icmp NUM</i>}] [srcport <i>PORT</i>{-<i>PORT</i>}] [dstport <i>PORT</i>{-<i>PORT</i>}] [duration <i>NUM</i>]] iddel <i>NODE_ID ID</i> flush </pre>	<p>Can be used to view, add, or delete active blacklist entries. The blacklist is applied as defined in Access Rules.</p> <p>Commands:</p> <p>show displays the current active blacklist entries in format: engine node ID blacklist entry ID (internal) entry creation time (internal) address and port match originally set duration (internal) (internal). Use the -f option to specify a storage file to view (<code>/data/blacklist/db_<number></code>). The -v option adds operation's details to the output.</p> <p>add creates a new blacklist entry. Enter the parameters (see below) or use the -i option to import parameters from a file.</p> <p>del deletes the first matching blacklist entry. Enter the parameters (see below) or use the -i option to import parameters from a file.</p> <p>iddel <i>NODE_ID ID</i> removes one specific blacklist entry on one specific engine. <i>NODE_ID</i> is the engine's ID, <i>ID</i> is the blacklist entry's ID (as shown by the show command).</p> <p>flush deletes all blacklist entries.</p> <p>Add/Del Parameters:</p> <p>Enter at least one parameter. The default value is used for the parameters that you omit. You can also save parameters in a text file; each line in the file is read as one blacklist entry.</p> <p>src <i>IP_ADDRESS/MASK</i> defines the source IP address and netmask to match. Matches any IP address by default.</p> <p>dst <i>IP_ADDRESS/MASK</i> defines the destination IP address and netmask to match. Matches any IP address by default.</p> <p>proto {<i>tcp udp icmp NUM</i>} defines the protocol to match by name or protocol number. Matches all IP traffic by default.</p> <p>srcport <i>PORT</i>[-<i>PORT</i>] defines the TCP/UDP source port or range to match. Matches any port by default.</p> <p>dstport <i>PORT</i>[-<i>PORT</i>] defines the TCP/UDP destination port or range to match. Matches any port by default.</p> <p>duration <i>NUM</i> defines in seconds how long the entry is kept. Default is 0, which cuts current connections, but is not kept.</p> <p>Examples:</p> <pre> sg-blacklist add src 192.168.0.2/32 proto tcp dstport 80 duration 60 sg-blacklist add -i myblacklist.txt sg-blacklist del dst 192.168.1.0/24 proto 47 </pre>

Table A.1 StoneGate-specific Command Line Tools on Engines (Continued)

Command	Description
<pre> sg-bootconfig [--primary-console=<i>tty0/ttyS</i> <i>PORT,SPEED</i>] [--secondary-console= [<i>tty0/ttyS</i> <i>PORT,SPEED</i>]] [--flavor=<i>up/smp</i>] [--initrd=<i>yes/no</i>] [--crashdump=<i>yes/no/Y@X</i>] [--append=<i>kernel options</i>] [--help] apply </pre>	<p>Can be used to edit boot command parameters for future bootups.</p> <p>--primary-console=<i>tty0/ttyS PORT,SPEED</i> parameter defines the terminal settings for the primary console.</p> <p>--secondary-console= [<i>tty0/ttyS PORT,SPEED</i>] parameter defines the terminal settings for the secondary console.</p> <p>--flavor=<i>up/smp [-kdb]</i> parameter defines whether the kernel is uniprocessor or multiprocessor.</p> <p>--initrd=<i>yes/no</i> parameter defines whether Ramdisk is enabled or disabled.</p> <p>--crashdump=<i>yes/no/Y@X</i> parameter defines whether kernel crashdump is enabled or disabled, and how much memory is allocated to the crash dump kernel (Y). The default is 24M. X must always be 16M.</p> <p>--append=<i>kernel options</i> parameter defines any other boot options to add to the configuration.</p> <p>--help parameter displays usage information.</p> <p>apply command applies the specified configuration options.</p>
<pre> sg-clear-all </pre>	<p>Use this only if you want to return a StoneGate appliance to its factory settings.</p> <p>Clears all configuration from the engine. You must have a serial console connection to the engine to use this command.</p>
<pre> sg-contact-mgmt </pre>	<p>Used for establishing a trust relationship with the Management Server as part of engine installation or reconfiguration (see <i>sg-reconfigure</i> below). The engine contacts the Management Server using the one-time password created when the engine's initial configuration is saved.</p>
<pre> sg-logger -f <i>FACILITY_NUMBER</i> -t <i>TYPE_NUMBER</i> [-e <i>EVENT_NUMBER</i>] [-i "<i>INFO_STRING</i>"] [-s] [-h] </pre>	<p>Can be used in scripts to create log messages with the specified properties.</p> <p>-f <i>FACILITY_NUMBER</i> parameter defines the facility for the log message.</p> <p>-t <i>TYPE_NUMBER</i> parameter defines the type for the log message.</p> <p>-e <i>EVENT_NUMBER</i> parameter defines the log event for the log message. The default is 0 (H2A_LOG_EVENT_UNDEFINED).</p> <p>-i "<i>INFO_STRING</i>" parameter defines the information string for the log message.</p> <p>-s parameter dumps information on option numbers to stdout</p> <p>-h parameter displays usage information.</p>

Table A.1 StoneGate-specific Command Line Tools on Engines (Continued)

Command	Description
<pre>sg-raid [-status] [-add] [-re-add] [-force] [-help]</pre>	<p>Configures a new hard drive on a StoneGate appliance. This command is only available for StoneGate appliances that support RAID (Redundant Array of Independent Disks) and have two hard drives.</p> <ul style="list-style-type: none"> -status option displays the status of the hard drive. -add options adds a new empty hard drive. Use -add -force if you want to add a hard drive that already contains data and you want to overwrite it. -re-add adds a hard drive that is already partitioned. This command prompts for the drive and partition for each degraded array. Use -re-add -force if you want to check all the arrays. -help option option displays usage information.
<pre>sg-reconfigure [--boot] [--no-shutdown]</pre>	<p>Used for reconfiguring the node manually.</p> <ul style="list-style-type: none"> --boot option applies bootup behavior. Do not use this option unless you have a specific need to do so. --no-shutdown option allows you to make limited configuration changes on the node without shutting it down. Some changes may not be applied until the node is rebooted.
<pre>sg-status [-l] [-h]</pre>	<p>Displays information on the engine's status.</p> <ul style="list-style-type: none"> -l option displays all available information on engine status. -h option displays usage information.
<pre>sg-toggle-active SHA1 SIZE --force [--debug]</pre>	<p>Switches the engine between the active and the inactive partition. This change takes effect when you reboot the engine. You can use this command, for example, if you have upgraded an engine and want to switch back to the earlier engine version. When you upgrade the engine, the active partition is switched. The earlier configuration remains on the inactive partition. To see the currently active (and inactive) partition, see the directory listing of <code>/var/run/stonegate</code> (<code>ls-l /var/run/stonegate</code>).</p> <p>The <code>SHA1 SIZE</code> option is used to verify the signature of the inactive partition before changing it to active. If you downgrade the engine, check the checksum and the size of the earlier upgrade package by extracting the signature and size files from the <code>sg_engine_[version.build]_i386.zip</code> file.</p> <ul style="list-style-type: none"> --debug option reboots the engine with the debug kernel. --force option switches the active configuration without first verifying the signature of the inactive partition.
<pre>sg-version</pre>	<p>Displays the software version and build number for the node.</p>

Table A.1 StoneGate-specific Command Line Tools on Engines (Continued)

Command	Description
sginfo [-f] [-d] [-s] [-p] [--] [--help]	Gathers system information you can send to Stonesoft support if you are having problems. Use this command only when instructed to do so by Stonesoft support. -f option forces sgInfo even if the configuration is encrypted. -d option includes core dumps in the sgInfo file. -s option includes slapcat output in the sgInfo file. -p option includes passwords in the sgInfo file (by default passwords are erased from the output). -- option creates the sgInfo file without displaying the progress --help option displays usage information.

General Tools

The table below lists some general operating system commands that may be useful in running your StoneGate engines. Some commands can be stopped by pressing Ctrl+c.

Table A.2 General Command Line Tools on Engines

Command	Description
dmesg	Shows system logs and other information. Use the -h option to see usage.
halt	Shuts down the system.
ip	Displays IP-address related information. Type the command without options to see usage. Example: type ip addr for basic information on all interfaces.
ping	Tool for sending ICMP echo packages to test connectivity. Type the command without options to see usage.
ps	Reports status of running processes.
reboot	Reboots the system. Upon reboot, you enter a menu with startup options. For example, this menu allows you to return the engine to the previous configuration.
scp	Secure copy. Type the command without options to see usage.
sftp	Secure FTP (for transferring files securely). Type the command without options to see usage.
ssh	SSH client (for opening a terminal connection to other hosts). Type the command without options to see usage.
tcpdump	Gives information on network traffic. Use the -h option to see usage.
top	Displays the top CPU processes taking most processor time. Use the -h option to see usage.

APPENDIX B

DEFAULT COMMUNICATION PORTS

This chapter lists the default ports used in connections between StoneGate components and the default ports StoneGate uses with external components.

The following sections are included:

- ▶ [Management Center Ports](#) (page 96)
- ▶ [IPS Engine Ports](#) (page 98)

Management Center Ports

The illustrations below present an overview to the most important default ports used in communications between the Management Center (SMC) components and from the SMC to external services. See the table below for a complete list of default ports.

ILLUSTRATION B.1 Destination Ports for Basic Communications Within SMC Management Client

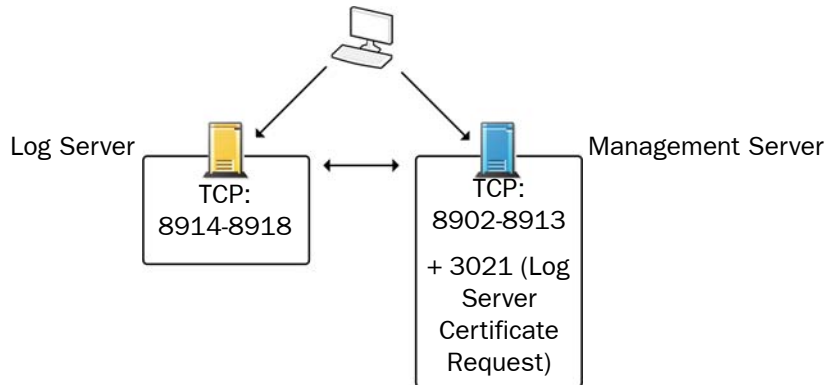
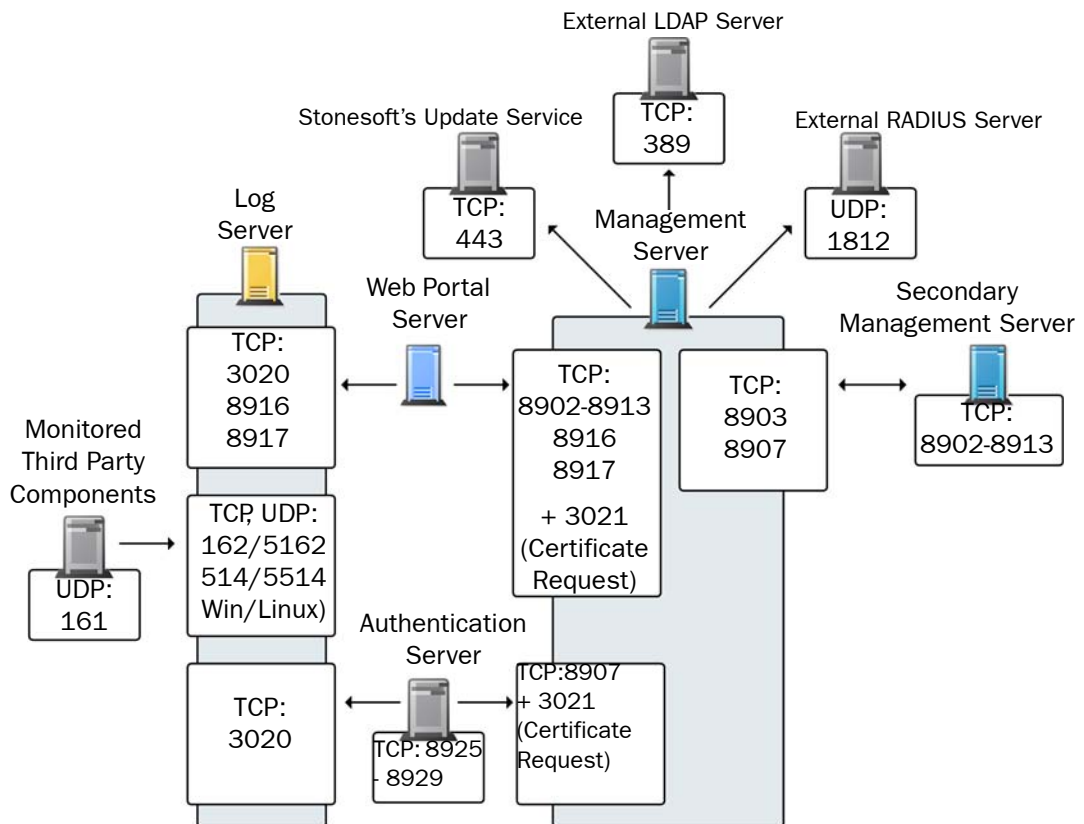


ILLUSTRATION B.2 Default Destination Ports for Optional SMC Components and Features



The table below lists all default ports SMC uses internally and with external components. Many of these ports can be changed. The name of corresponding default Service elements are also included for your reference. For information on communications between SMC components and the engines, see the separate listings.

TABLE B.1 Management Center Default Ports

Listening Host	Port/Protocol	Contacting Hosts	Service Description	Service Element Name
Authentication Server	8925-8929/TCP	Management Server	StoneGate Management Server commands to Authentication Server.	SG Authentication Commands
Authentication Server node	8988-8989/TCP	Authentication Server node	Data synchronization between Authentication Server nodes.	SG Authentication Sync
DNS server	53/UDP, 53/TCP	Management Client, Management Server, Log Server	DNS queries.	DNS (UDP)
LDAP server	389/TCP	Management Server	External LDAP queries for display/editing in the Management Client.	LDAP (TCP)
Log Server	162/UDP, 5162/UDP	Monitored third party components	SNMPv1 trap reception from third party components. Port 162 is used if installed on Windows, port 5162 if installed on Linux.	SNMP (UDP)
Log Server	514/TCP, 514/UDP, 5514/TCP, 5514/UDP	Monitored third party components	Syslog reception from third party components. Port 514 is used if installed on Windows, port 5514 if installed on Linux.	Syslog (UDP) [Partial match]
Log Server	3020/TCP	Authentication Server, Log Server, Web Portal Server	Alert sending.	SG Log
Log Server	8914-8918/TCP	Management Client	Log browsing.	SG Data Browsing
Log Server	8916-8917/TCP	Web Portal Server	Log browsing.	SG Data Browsing (Web Portal Server)
Management Server	3021/TCP	Log Server, Web Portal Server	System communications certificate request/renewal.	SG Log Initial Contact
Management Server	8902-8913/TCP	Management Client, Log Server, Web Portal Server	Monitoring and control connections.	SG Control
Management Server	8907/TCP	Authentication Server	Status monitoring.	SG Control

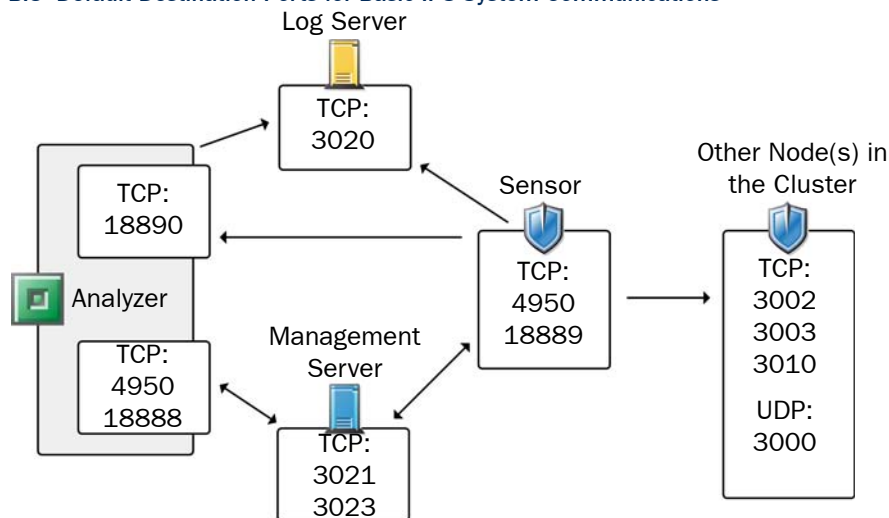
TABLE B.1 Management Center Default Ports (Continued)

Listening Host	Port/Protocol	Contacting Hosts	Service Description	Service Element Name
Monitored Third Party Components	161/UDP	Log Server	SNMP status probing to external IP addresses.	SNMP (UDP)
Primary Management Server	8903, 8907/TCP	Secondary Management Servers	Database replication (pull) to the secondary Management Server.	SG Control
RADIUS server	1812/UDP	Management Server	RADIUS authentication requests for administrator logins. The default ports can be modified in the properties of the RADIUS Server element.	RADIUS (Authentication)
Secondary Management Servers	8902-8913/TCP	Primary Management Server	Database replication (push) to the secondary Management Server.	SG Control
Stonesoft servers	443/TCP	Management Server	Update packages, engine upgrades, and licenses from update.stonesoft.com and smc.stonesoft.com.	HTTPS
Syslog Server	514/UDP, 5514/UDP	Log Server	Log data export to syslog servers. The default ports can be modified in the LogServerConfiguration.txt file.	Syslog (UDP) [Partial match]

IPS Engine Ports

The illustration below presents an overview to the most important default ports used in communications between IPS engines and the SMC and between clustered sensor engines. See the table below for a complete list of default ports.

ILLUSTRATION B.3 Default Destination Ports for Basic IPS System Communications



The table below lists all default ports StoneGate IPS uses internally and with external components. Many of these ports can be changed. The name of corresponding default Service elements are also included for your reference.

TABLE B.2 IPS-Specific Ports

Listening Hosts	Port/Protocol	Contacting Hosts	Service Description	Service Element Name
Analyzer	514/UDP	Syslog server	Syslog messages forwarded to Analyzer.	Syslog (UDP)
Analyzer	4950/TCP	Management Server	Remote upgrade.	SG Remote-Upgrade
Analyzer	18889/TCP	Management Server	Management connection.	SG Commands (Analyzer)
Analyzer	18890/TCP	Sensor	Event data sent from the Sensors.	SG Event Transfer
BrightCloud Server	2316/TCP	Sensor	BrightCloud web filtering update service.	BrightCloud update
Log Server	3020/TCP	Analyzer, Sensor	Log and alert messages from Analyzers; recording file transfers from Sensors; and monitoring of blacklists, status, and statistics from Sensors.	SG Log
Management Server	3021/TCP	Sensor, analyzer	System communications certificate request/renewal (initial contact).	SG Initial Contact
Management Server	3023/TCP	Sensor, analyzer	Backup monitoring (status) connection.	SG Reverse Monitoring

TABLE B.2 IPS-Specific Ports (Continued)

Listening Hosts	Port/Protocol	Contacting Hosts	Service Description	Service Element Name
Sensor	3000-3001/ UDP 3002,3003, 3010/TCP	Sensor	Heartbeat between the cluster nodes.	SG State Sync (Multicast), SG State Sync (Unicast), SG Data Sync
Sensor	4950/TCP	Management Server	Remote upgrade.	SG Remote Upgrade
Sensor	18888/TCP	Management Server	Management connection.	SG Commands (Sensor)
Sensor, firewall	15000/TCP	Management Server, analyzer, sensor	Blacklist entries.	SG Blacklisting

APPENDIX C

EXAMPLE NETWORK SCENARIO

To give you a better understanding of how StoneGate fits into a network, this section outlines a network with IPS Sensors and Analyzers.

All illustrations of the software configuration in the subsequent chapters are filled in according to this example scenario; this way, you can compare how the settings in the various dialogs relate to overall network structure whenever you like.

The following sections are included:

- ▶ [Overview of the Example Network](#) (page 102)
- ▶ [Example Headquarters Intranet Network](#) (page 103)
- ▶ [Example Headquarters Management Network](#) (page 104)
- ▶ [Example Headquarters DMZ Network](#) (page 105)
- ▶ [Example Branch Office Network](#) (page 106)

Overview of the Example Network

Three example Sensor installations are described in this Guide:

- a Sensor cluster in the Headquarters Intranet network.
- a single Sensor in the Headquarters DMZ network.
- a combined Sensor-Analyzer in the Branch Office Intranet network.

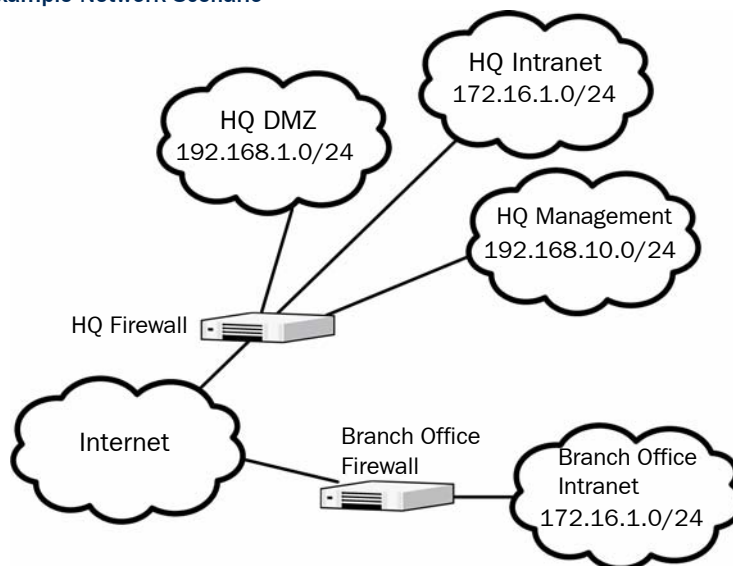
The two different Analyzer installations are illustrated with

- a separate Analyzer in the Headquarters Management Network.
- a combined Sensor-Analyzer in the Branch Office Intranet network.

The network scenario for these installations is based on the example network in [Illustration C.1](#).

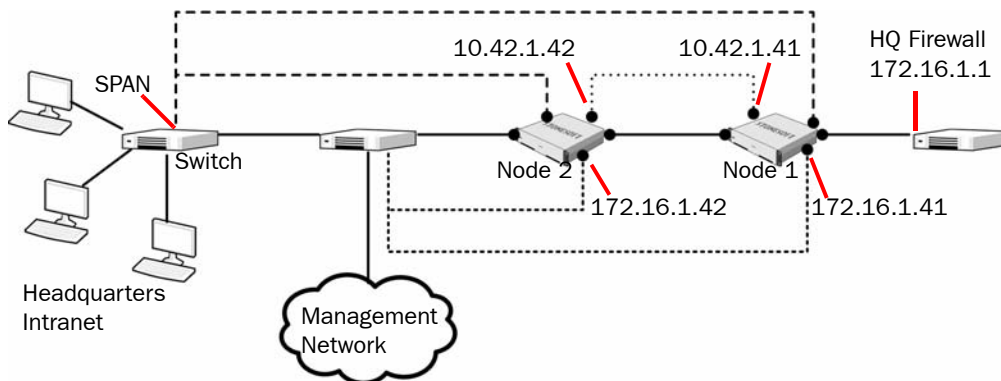
See the *IPS Reference Guide* for more information on deploying the StoneGate IPS components.

Illustration C.1 Example Network Scenario



Example Headquarters Intranet Network

Illustration C.2 Example Headquarters Intranet Network



HQ Sensor Cluster

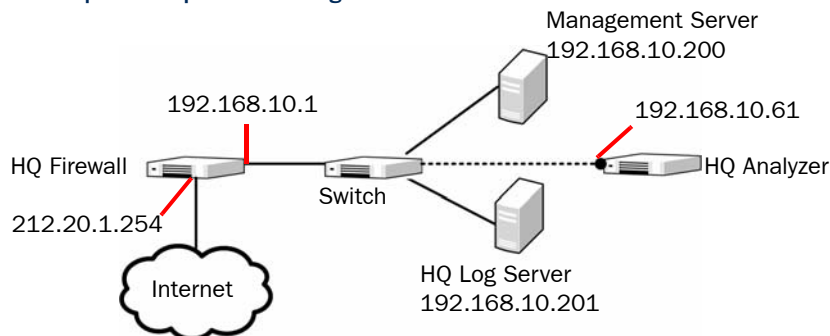
In the example scenario, *HQ Sensor Cluster* is an inline serial cluster located in the Headquarters network. The cluster consists of two Sensor nodes: *Node 1* and *Node 2*.

Table C.1 Sensor Cluster in the Example Scenario

Network Interface	Description
Capture Interfaces	The HQ Sensor Cluster's Capture Interface on each node is connected to a SPAN port in the Headquarters Intranet switch. All the traffic in this network segment is forwarded to the SPAN ports for inspection.
Inline Interfaces	The cluster is deployed in the path of traffic between the firewall and the Headquarters Intranet switch. All the traffic flows through each node's inline interface pair.
Normal Interfaces	The normal interface on each node is connected to the Headquarters Intranet switch. Node 1's IP address is 172.16.1.41 and Node 2's address is 172.16.1.42. This normal interface is used for control connections from the Management Server, sending events to the HQ Analyzer, and for sending TCP resets.
Heartbeat interfaces	The nodes have dedicated heartbeat interfaces. Node 1 uses the IP address 10.42.1.41 and Node 2 uses the IP address 10.42.1.42.

Example Headquarters Management Network

Illustration C.3 Example Headquarters Management Network



HQ Analyzer

The HQ Analyzer receives event data from the DMZ Sensor and from the HQ Sensor Cluster, and sends log data and alerts to the HQ Log Server.

Table C.2 Analyzer in the Example Scenario

Network Interface	Description
Normal Interfaces	The HQ Analyzer's normal interface is connected to the Headquarters' Management Network using the IP address 192.168.10.61. This normal interface is used for control connections from the Management Server, receiving event information from the sensors, sending log data and alerts, and sending IP Blacklists to the defined firewalls.

HQ Firewall

The HQ Firewall provides NAT for the Headquarters Management network. The HQ Firewall uses the following IP addresses with the Headquarters Management Network:

- Internal: 192.168.10.1
- External: 212.20.1.254

Management Center Servers

Table C.3 SMC Servers in the Example Scenario

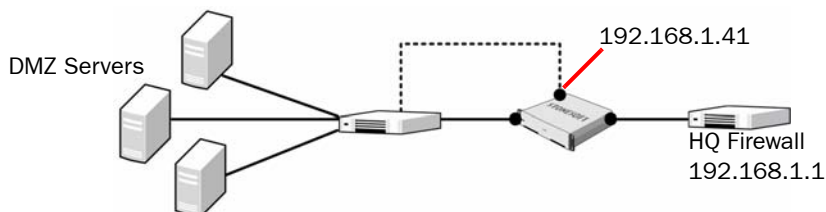
SMC Server	Description
Management Server	The Management Server in the Headquarters' Management Network with the IP address 192.168.10.200. This Management Server manages all the StoneGate IPS Sensors, Analyzers, and Log Servers of the example network.

Table C.3 SMC Servers in the Example Scenario (Continued)

SMC Server	Description
HQ Log Server	This server is located in the Headquarters' Management Network with the IP address 192.168.10.201. This Log Server receives alerts and log data from the HQ Analyzer.

Example Headquarters DMZ Network

Illustration C.4 Example Headquarters DMZ Network



DMZ Sensor

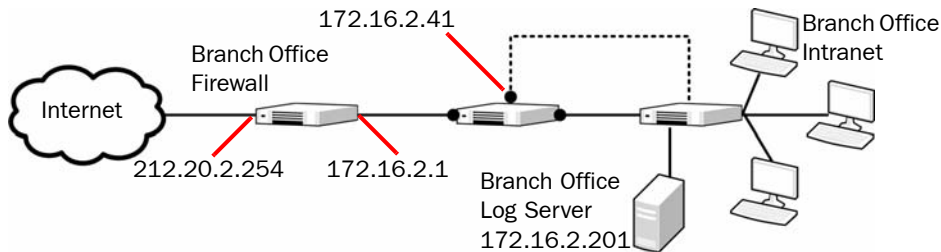
In the example scenario, the *DMZ Sensor* in the Headquarters DMZ network is a single inline Sensor.

Table C.4 Single Sensor in the Example Scenario

Network Interface	Description
Inline Interfaces	The DMZ Sensor is deployed in the path of traffic between the firewall and the DMZ network switch. All the traffic flows through the sensor's inline interface pair.
Normal Interfaces	The normal interface is connected to the DMZ network using the IP address 192.168.1.41. This normal interface is used for control connections from the Management Server, sending event information to the HQ Analyzer, and for TCP connection termination.

Example Branch Office Network

Illustration C.5 Example Branch Office Network



Branch Office Sensor-Analyzer

In the example scenario, the *Branch Office Sensor-Analyzer* is an inline combined Sensor-Analyzer.

Table C.5 Combined Sensor-Analyzer in the Example Scenario

Network Interface	Description
Inline Interfaces	The Branch Office Sensor-Analyzer is deployed in the path of traffic between the firewall and the Branch Office Intranet switch. All the traffic flows through the sensor's inline interface pair.
Normal Interfaces	The Branch Office Sensor-Analyzer has one normal interface that is connected to the Branch Office Intranet using the IP address 172.16.2.41. This normal interface is used for control connections from the Management Server, sending log data and alerts to the Branch Office Log Server, and for TCP connection termination (by the Sensor).

Branch Office Firewall

The Branch Office Firewall provides NAT for the Branch Office network. The Branch Office Firewall has the following IP addresses:

- Internal: 172.16.2.1
- External: 212.20.2.254

Branch Office Log Server

In the example scenario, the *Branch Office Log Server* is located in the Branch Office Intranet with the IP address 172.16.2.201. This Log Server receives alerts and log data from the Branch Office Sensor-Analyzer.

INDEX

- A**
 - activating initial configuration, 68
 - Advanced Configuration and Power Interface (ACPI), 62
 - analyzers
 - configuring, 31–44
 - installing, 62–71
 - Automatic Power Management (APM), 62
- B**
 - BIOS settings, 62
- C**
 - capture interfaces, 41
 - certification policy, 55
 - checking engine version, 76
 - checking file integrity, 77
 - checksums, 62–63
 - command line tools, 89
 - compatibility
 - network devices, 16
 - platforms supported, 15
 - contact addresses, 26–27
 - contact information, 10
 - customer support, 10
- D**
 - date and time settings, 15
 - deployment example, 101
 - documentation available, 9
- E**
 - engine commands, 90
 - engine configuration
 - analyzer, 64–70
 - sensor, 64–70
 - engine installation
 - in expert mode, 70
 - on intel and compatible, 61–71
 - engine interfaces
 - capture interfaces, 41
 - inline interfaces, 42
 - interface options, 37
 - IP addresses, 36
 - logical interfaces, 39
 - physical interfaces, 34
 - reset interfaces, 40
 - system communication interfaces, 33
 - traffic inspection interfaces, 38
 - VLANs, 35
 - example network scenario, 14, 101
- F**
 - file integrity, 62–63
- G**
 - generating licenses, 20
- H**
 - hardware requirements, 10
- I**
 - IDS (intrusion detection system), 14
 - importing licenses, 80–81
 - initial bypass state, 67
 - initial configuration
 - activating, 68
 - importing, 65
 - saving, 45–49
 - inline interfaces, 42
 - installation files, 62
 - installation procedure, 15
 - installation types for sensors, 14
 - integrity of files, 62–63
 - interface ID numbering, 32
 - IPS (intrusion prevention system), 14
 - IPS policies
 - certification policy, 55
 - strict policy, 55
 - system policy, 55
- L**
 - licenses, 19–22
 - checking, 21
 - generating, 20
 - installing, 80–81
 - upgrading, 78–81
 - locations, 25–26
 - log server contact addresses, 26–27
 - logical interfaces, 39
- M**
 - management server contact addresses, 26–27
 - MD5 checksum, 62–63
 - mirroring ports, 16
- N**
 - NAT (network address translation), 23–27
- O**
 - one-time password, 69
 - overview to the installation, 15

P

- partitioning hard disk manually, 70
- planning installation, 13–17
- platforms supported, 15
- policies, 51–58
 - strict policy, 55
 - system policy, 55
- ports, 16

R

- requirements for hardware, 10
- reset interfaces, 40
- routing, 52–55

S

- saving initial configuration, 45–49
- sensor installation types, 14
- sensors
 - configuring, 31–44
 - installing, 62–71
 - traffic inspection interfaces, 38–44
- SHA-1 checksum, 62–63
- sniffing network interface, 67
- SPAN port, 16
- strict policy, 55
- support services, 10
- supported platforms, 15
- system policy, 55
- system requirements, 10

T

- TAP, 16
- technical support, 10
- traffic inspection interfaces
 - capture interfaces, 41
 - inline interfaces, 42
 - logical interfaces, 39
 - reset interfaces, 40
- transferring initial configuration to engines, 49
- typographical conventions, 8

U

- upgrading, 75–86
 - engine locally, 84
 - engine remotely, 82
 - licenses, 78–81

W

- wire TAP, see TAP

StoneGate Guides

Administrator's Guides - step-by-step instructions for configuring and managing the system.

Installation Guides - step-by-step instructions for installing and upgrading the system.

Reference Guides - system and feature descriptions with overviews to configuration tasks.

User's Guides - step-by-step instructions for end-users.

For more documentation, visit
www.stonesoft.com/support/

Stonesoft Corporation

Itälahdenkatu 22 A
FI-00210 Helsinki
Finland

Tel. +358 9 476 711
Fax +358 9 4767 1349

STONESOFT

Secure Information Flow

Stonesoft Inc.

1050 Crown Pointe Parkway
Suite 900
Atlanta, GA 30338
USA

Tel. +1 770 668 1125
Fax +1 770 668 1131